**UNIVERSIDAD CARLOS III**

**Escuela Politécnica Superior**


Ingeniería Técnica en Informática de Gestión

# PROYECTO FIN DE CARRERA

## Sistema de gestión remota basada en la tecnología Intel vPro para entornos corporativos

**Autor:** Álvaro Guijarro Hernando

**Tutor:** Francisco Javier García Blas

**Marzo 2013**

# Resumen

Toda empresa tiene que enfrentarse, necesariamente, a la gestión de su flota de ordenadores. Esta tarea es fundamental para mantener los equipos actualizados y controlados por el departamento de TI. La gestión remota de todos ellos permite un significativo ahorro de costes, esfuerzo, tiempo y energía, ya que permite evitar el desplazamiento del personal cualificado al lugar donde se encuentra el equipo afectado, además del tiempo en el que los equipos no son funcionales, derivando en una pérdida de capacidad productiva.

En este caso, estudiaremos cómo se ha podido llevar a cabo un proyecto de gestión remota de una red de ordenadores, accediendo a ellos independientemente de su estado (fuera de banda, apagado…) y aislados de la red corporativa. Para ello, se ha utilizado la tecnología *Fast Call For Help* de Intel que, al contrario que muchas otras alternativas de gestión remota, permite que sea el cliente el que establezca el primer contacto con el departamento de TI solicitando ayuda. Esto permite que se cree una ruta punto a punto para poder establecer una conexión desde la consola de gestión hasta el cliente, sin importar que se encuentre fuera de la red corporativa.

A lo largo de este Proyecto Fin de Carrera, compararemos las tecnologías de las que dispondremos para solucionar el problema planteado, elegiremos una de ellas, definiremos los distintos componentes que serán necesarios para implementarla, los configuraremos, haremos pruebas y valoraremos el trabajo realizado.

Ha sido necesario reproducir un entorno adecuado para la implantación de esta tecnología. Para ello ha sido necesario definir tres zonas claramente diferenciadas:

zona cliente, que representará un equipo gestionado por el administrador de TI.

zona desmilitarizada (DMZ), donde se instalará el servidor web necesario, el túnel seguro “Stunnel” y el MPS (*Management Presence Server*), y

zona de consola, consistente en el equipo que tendrá instalada la consola de gestión para resolver las incidencias, la cual controlará el administrador de TI.

# Abstract

Every company necessarily has to deal the management of its computers. This is essential to keep them updated and controlled by the IT department. Remote management of the computer infrastructure allows a significant cost, effort, time and energy savings.

In this case, we will study how it was possible to carry out a project of remote management of a computer network, gaining access to the computers regardless of their status (in/out of bounds, powered on/off) and isolated from the corporate network. For this, we used the Intel Fast Call For Help technology that, unlike many other remote management options, it allows the client to establish first contact with the IT department for help wherever it is. This allows the infrastructure to create a route point-to-point in order to establish a connection from the management console to the client, even if the client is outside the corporate network.

It was necessary to reproduce a suitable environment for the implementation of this technology. This has involved three distinct areas:

client area, where all the managed PCs will be allocated

DeMilitarized Zone (DMZ), where the web server, Stunnel and MPS (Management Presence Server) will be installed, and finally,

console part, where the console software will be installed for the IT admin to manage the PCs.

# Índice general

# Índice de tablas

# Índice de ilustraciones

# **Capítulo 1.** Introducción

El objetivo de este capítulo es presentar el trabajo realizado en este Proyecto Fin de Carrera y describir la estructura de este documento. Con esta introducción, se describirá el problema que se plantea, los motivos que han llevado al desarrollo de una solución, su análisis y los objetivos que se desean alcanzar.

La gestión remota permite al departamento de TI el control a distancia del sistema que requiera asistencia, permitiendo operar con él sin encontrarse en el mismo lugar para resolver incidencias, actualizar o instalar software, etc.

Podemos distinguir tres tipos de gestión remota: la gestión de incidencias, de hardware y de software.

Ante un incidente imprevisto, la gestión remota de incidencias se ocupa de recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan. Permite al servicio técnico no tener que desplazarse hasta el lugar donde se ha producido la interrupción del servicio, obteniendo el control del sistema y pudiendo emitir un diagnóstico a distancia. Normalmente, esta gestión es administrada por el servicio técnico de la empresa. El objetivo de la gestión de incidencias es recuperar el normal funcionamiento lo más rápido posible con el menor impacto, tanto en el negocio como en el usuario, con un coste óptimo.

**Ilustración 1. Representación de gestión remota**

A su vez, las incidencias pueden tener ser de varios tipos. Entre ellos se encuentran las incidencias hardware (fallos de componentes físicos que posiblemente requieran una sustitución de la pieza: fallos causados por una avería eléctrica, un cortocircuito, un pico de tensión, una mala conexión entre contactos…), software (drivers corruptos o desactualizados, errores de código en aplicaciones, librerías o componentes del sistema operativo corruptos, etc.), de seguridad (antivirus desactualizado, vulneración del sistema, brechas de seguridad…) o de virus (infecciones que pueden causar mayores o menores daños, dependiendo del tipo de amenaza detectada).

La gestión de hardware puede ser muy beneficiosa a la hora de diagnosticar problemas en las piezas que integran los equipos. Con ello se consigue, además de detectar posibles incompatibilidades entre las piezas de hardware que los componen, determinar la marca, modelo o número de serie y reemplazar la pieza defectuosa (en su caso) por otra de igual o de similares características, para asegurar el correcto funcionamiento. También es útil para detectar qué equipos son los que tienen el hardware más antiguo y establecer prioridades si la empresa decidiera establecer un plan de renovación de su flota de equipos informáticos.

La gestión del software permite tener un mayor control sobre los componentes lógicos instalados en los equipos de la empresa. Esto consiste en la posibilidad de tener un inventario software de cada uno de los equipos con el objetivo de monitorizar qué programas están o no instalados en el ordenador del usuario y para poder identificar posibles problemas por incompatibilidades, verificar qué versiones de dichos programas están instaladas, etc. También es útil para gestionar el "parcheado", tanto del sistema operativo para tapar posibles agujeros de seguridad o mejoras en el rendimiento, como de las aplicaciones que estén instaladas para implementar nuevas

características. Además, la distribución de aplicaciones puede ser una herramienta muy útil para los administradores de TI a la hora de querer implantar un nuevo programa en toda la red de ordenadores. En lugar de tener que instalar los programas uno a uno en todos los equipos, con el posible gasto innecesario de tiempo, costes de desplazamiento y recursos que eso conllevaría, se puede hacer mediante una consola de gestión que tenga esa capacidad. De esta manera, además de hacer el proceso más cómodo y rápido, supone un ahorro para la empresa en comparación con la gestión de incidencias de forma presencial.

Entre los mayores beneficios de la gestión remota tenemos el mencionado ahorro de costes (coste de productividad, de operación, de energía), y un aumento de la flexibilidad (perfiles de usuario, imágenes de los Sistemas Operativos, etc.).

## 1.1. Motivación del Proyecto

Hoy en día, la inmensa mayoría de las empresas se apoyan en las tecnologías para llevar a cabo su actividad diaria. Es por ello que requieren de una serie de equipos informáticos usados por los empleados funcionando continuamente para poder mantener un entorno productivo. Cuando este ritmo se interrumpe, se producen pérdidas en tiempo y en dinero para la empresa, y por ello es necesario restablecer la actividad lo antes posible. Además, el problema es todavía mayor si dicha avería se producía en un equipo cliente que estuviera fuera de la red corporativa, lo que dificultaba el acceso al mismo y por lo tanto aumentaba el tiempo de vuelta al estado productivo del equipo.

Hasta ahora, dichas incidencias se tenían que solucionar, bien por la presencia física de un técnico cualificado delante del equipo averiado, o bien a través de acceso remoto, siempre que la avería se produjera en un entorno en el que se pudiera establecer una conexión remota. Por ejemplo, dentro del sistema operativo.

En este sentido, el poder prescindir del desplazamiento del técnico al lugar de la incidencia, con el coste de tiempo y de dinero que esto implica, significa un avance importante. Si bien existe una extensa gama de herramientas y tecnologías para administrar de forma remota los sistemas que están encendidos (en banda) con un sistema operativo que responde (en servicio), la lista de opciones de administración disminuye significativamente cuando los clientes están apagados (fuera de banda) o cuando tienen un sistema operativo que no responde (fuera de servicio).

En este Proyecto Fin de Carrera se abordará el modo de conseguir diagnosticar y, en gran medida, solucionar las incidencias de un equipo cliente independientemente de si se encuentra dentro o fuera de la red corporativa, siempre que cuente con una conexión de red. Con ello se consigue diagnosticar la causa de la incidencia y proceder a su solución de forma más rápida.

## 1.2. Objetivos

La intención de este Proyecto Fin de Carrera es describir e implementar un conjunto de herramientas que permitan establecer conexiones remotas a equipos pertenecientes a una misma organización empresarial pero que no se encuentren físicamente dentro del mismo ámbito con el fin de diagnosticar averías o incidencias de forma no presencial.

Con esta solución se pondrá fin al problema que planteaba el hecho de que se produjera alguna incidencia en el equipo informático de un empleado si estuviera en un viaje por motivos de trabajo, o en una reunión fuera de su empresa, o simplemente en cualquier entorno fuera del alcance físico del departamento de TI.

## 1.3. Estructura del documento

El Proyecto está dividido en varios capítulos, agrupados de forma lógica de tal modo que a través de lectura ordenada se consiga la comprensión paulatina y global del problema planteado y su solución:

- En el Capítulo 1, **INTRODUCCIÓN**, se establece el marco en el que nos situaremos, la motivación que nos ha llevado a realizarlo y la presentación de sus objetivos.

- En el Capítulo 2, **ESTADO DE LA CUESTIÓN**, se presenta una visión global de las tecnologías disponibles, estándares y otros elementos utilizados, además de una evaluación comparativa para elegir una solución concreta y los distintos motivos que justifican dicha decisión.

- En el Capítulo 3, **ANÁLISIS Y DISEÑO DE LA SOLUCIÓN**, se ofrece una explicación sobre qué solución se ha escogido y de qué elementos se compone, así como los distintos tipos de requisitos necesarios para implantarlo con éxito. Además, se explica de una manera técnica el entorno y cada uno de sus componentes, explicando el funcionamiento de cada una de las partes en las que se divide la solución.

- En el Capítulo 4, **IMPLANTACIÓN**, se explica paso a paso la puesta en marcha de la solución en un entorno real, especificando las herramientas software utilizadas y configurando cada una de ellas.

- En el Capítulo 5, **PRUEBAS**, se muestra la batería de pruebas a las que se someterá el entorno, así como los requisitos de cada una y sus resultados.

- En el Capítulo 6, **GESTIÓN DEL PROYECTO**, se comenta la metodología de trabajo, la planificación y el presupuesto.

- En el Capítulo 7, **CONCLUSIONES**, se presentan los comentarios adicionales al trabajo realizado, así como su valoración y posibles mejoras como trabajos futuros.

- En la **BIBLIOGRAFÍA** se incluye todos los documentos y páginas web utilizadas como referencia para la elaboración de este Proyecto.

- En el **APÉNDICE I** se incluye un completo glosario de términos, abreviaturas y acrónimos utilizados a lo largo del documento y necesarios para la comprensión del mismo.

- En el **APÉNDICE II** hay un listado de las consolas de gestión más relevantes que servirían como alternativas de pago a la utilizada en este Proyecto.

# Capítulo 2. Estado de la cuestión

En este capítulo definiremos los elementos necesarios para implantar una solución al problema de la gestión remota. Habrá que introducir elementos que permitan la conexión entre el cliente y la consola de gestión, así como certificados digitales que aseguren que la comunicación entre ambos extremos es segura. Además, plantearemos y compararemos las principales opciones disponibles actualmente para implantar el sistema de gestión remota y justificaremos las tecnologías escogidas para la correcta realización de este Proyecto Fin de Carrera.

## 2.1. Apache

El servidor Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows y Macintosh, entre otras, que implementa el protocolo HTTP/1.12.

De cara a este Proyecto, el objetivo del Servidor HTTP Apache es el de recibir las llamadas de los clientes para pasarlas a la consola de gestión, controlada por el administrador de TI.

En un principio Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA, ya que se trataba de una modificación sobre el mismo. Pero finalmente se rehízo en su versión 2.0 creándose un proyecto colaborativo de desarrollo en el que los voluntarios trabajan por ofrecer nuevos servicios y mejorar las presentes. Esto favorece a la resolución de las vulnerabilidades encontradas para las

que salen nuevas actualizaciones periódicamente, haciendo cada vez más seguro este tipo de servidor.

Entre sus características más importantes se encuentran las siguientes:

- Fácil y plena configuración de bases de datos de autenticación y negociado de contenido.

- Soporte a IPv6, la próxima generación de formato de direcciones IP.

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años.

## 2.2. Elementos de seguridad

Para poder implementar correctamente la solución necesitaremos disponer de ciertos elementos de seguridad que garanticen la comunicación segura entre los clientes (que se encontrarán fuera de la red corporativa) y la consola de gestión, que estará dentro de las instalaciones físicas de la empresa.

A continuación describiremos los componentes software que permitirán dicha transmisión segura de datos.

### 2.2.1. Stunnel

Stunnel es un programa multiplataforma y de código libre que permite cifrar conexiones TCP mediante SSL (Secure Sockets Layer) para se puedan comunicar dos extremos a través de un canal seguro. Stunnel utiliza criptografía de clave pública con el estándar X.509 para asegurar la conexión SSL.

Stunnel será útil para establecer un túnel seguro entre la empresa y el cliente que se encuentre fuera de ella, de manera que la comunicación entre ambos extremos esté cifrada.

### 2.2.2. Certificados

A continuación pasaremos a definir los distintos conceptos necesarios para entender cómo funcionan los certificados digitales y de qué manera ayudarán a implementar la solución al problema que plantea el Proyecto.

**¿Qué es el cifrado?**

El cifrado es un proceso matemático utilizado para codificar y decodificar información. El cifrado garantiza que la información permanezca oculta durante su transferencia, de manera que sólo el destinatario deseado pueda decodificarla. El número de bits (40, 56, 128 o 256 bits) indica el tamaño de la clave. Al igual que una contraseña más larga, una clave de mayor longitud ofrece un mayor número de combinaciones posibles. De hecho, el cifrado de 128 bits es un billón de billones de veces más potente que el cifrado de 40 bits. A modo de ejemplo ilustrativo, con las velocidades actuales de los ordenadores, alguien que tuviese a su disposición el tiempo, las herramientas y la motivación que se necesitan, tardaría un billón de años en descifrar una sesión que utilizase el cifrado de 128 bits. Los certificados SSL con criptografía activada por servidor (SGC, *Server-Gated Cryptography*) permiten utilizar un cifrado de 128 o 256 bits para la inmensa mayoría de los usuarios de Internet.

**El estándar X.509**

En criptografía, se usa para infraestructuras de claves públicas (*PKI* o *Public Key Infrastructure*). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. Su sintaxis, se define empleando el lenguaje ASN.1 (Abstract Syntax Notation One), y los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail), aunque en el caso de este Proyecto he utilizado exclusivamente éste último.

Al utilizar la comunicación por el protocolo SSL, es necesario disponer de unos certificados para asegurar que la transmisión de datos es confiable y discurren por un canal seguro.

Los certificados SSL permiten que se forme un lazo de confianza cliente-proveedor protegiendo los datos del cliente mediante su cifrado y dejando disponible el acceso a la información sólo mediante claves.

Los certificados SSL deben ser emitidos partiendo de un Certificado Raíz de una Autoridad de Certificación (CA, por sus siglas en inglés *Certificate Authority*) reconocida para que ésta indique que la conexión es de confianza.

## ¿Qué es Secure Sockets Layer (SSL)?

*Secure Sockets Layer* (SSL) es un protocolo de seguridad que usan, principalmente, los navegadores y los servidores web para ayudar a los usuarios a proteger sus datos durante las transferencias. Un certificado SSL contiene una clave pública e información de identificación verificada. En una conexión SSL, el servidor comparte su clave pública con el cliente para establecer un método de cifrado y una clave de cifrado única para esa sesión. El cliente confirma que reconoce al emisor del certificado SSL y que confía en él. Este proceso se conoce como el "protocolo de enlace de SSL" y da comienzo a una sesión segura que protege la privacidad de los participantes y la integridad de los mensajes.

## ¿Qué es la autenticación y por qué es importante para el SSL?

La autenticación es una verificación de la identidad llevada a cabo por un tercero a fin de establecer la confianza. Los certificados SSL se emiten de manera única para un determinado dominio y servidor web.

Para ello se tiene que pedir a una Autoridad de Certificación los ficheros correspondientes, con su correspondiente coste económico, pero para este Proyecto usaremos unos de prueba.

Necesitaremos un certificado primario o de servidor para el MPS (*Management Presence Server*), una clave privada para el MPS y un certificado raíz. Un certificado intermedio sería opcional si el entorno lo requisiera.

## ¿Qué es un certificado SSL?

Un certificado SSL es un archivo digital (o un pequeño trozo de código) que tiene dos funciones concretas:

1. Autenticación y verificación:

   El certificado SSL tiene información sobre la autenticidad de ciertos detalles de la identidad de una persona, negocio o sitio web, que se mostrará a los visitantes en la página web cuando hagan clic en el símbolo del candado o similar (por ejemplo, el sello de VeriSign).

**2.** Cifrado de datos:

El certificado SSL también permite el cifrado de datos, lo que significa que una información delicada que se intercambia a través de la web no podrá ser leída por nadie que no sea el destinatario legítimo de dicha información.

De mismo modo en que un documento de identidad físico sólo debe ser emitido por las autoridades gubernamentales pertinentes de cada país, un certificado SSL será más confiable si lo ha emitido una Autoridad de Certificación confiable. Las CAs tienen que seguir reglas y políticas muy estrictas sobre quién podrá o no podrá recibir un certificado digital SSL, así que cuando se posee uno, hay un nivel mucho más alto de confiabilidad.

**¿Qué es un certificado intermedio?**

Un certificado intermedio es un certificado digital que se ubica entre el certificado de servidor y un certificado raíz (normalmente instalado en el dispositivo del usuario). Un certificado intermedio es parte de una cadena de certificados.

Algunas organizaciones delegan la responsabilidad de la emisión de certificados para resolver el problema de la separación geográfica entre las unidades de la organización o para aplicar diferentes directivas de emisión a las diferentes secciones de la organización.

Es posible configurar Autoridades de Certificación subordinadas para delegar la responsabilidad de la emisión de certificados. El estándar X.509 incluye un modelo para la configuración de una jerarquía de CA. En este modelo, la CA raíz se encuentra en la parte superior de la jerarquía y cuenta con un certificado autofirmado. Las CA que dependen directamente de la CA raíz cuentan con certificados de la CA firmados por la CA raíz. Las CA que pertenecen a las CA subordinadas en la jerarquía cuentan con certificados de CA firmados por las CA subordinadas.

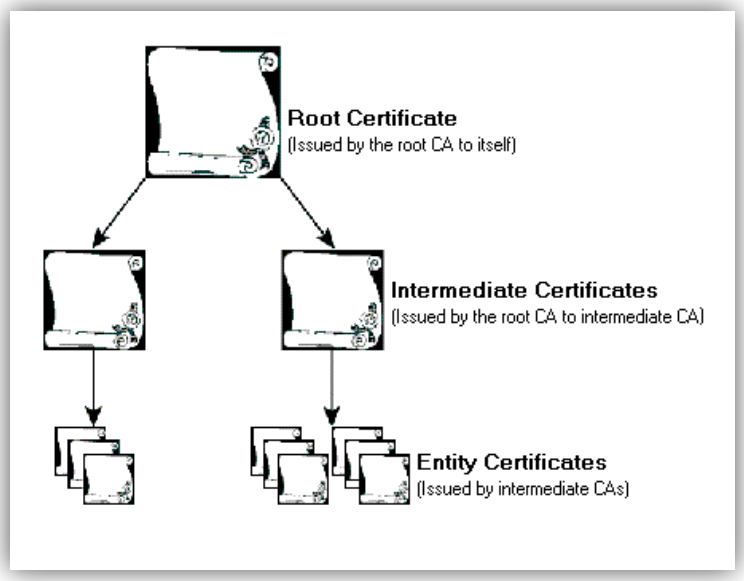



**Ilustración 2. Ejemplo de jerarquía de certificados digitales**

### ¿Cómo funciona el cifrado SSL?

De la misma manera que se abre y se cierra una puerta con una llave, el cifrado permite bloquear y desbloquear información. Si no disponemos de la llave necesaria, no seremos capaces de abrir la puerta, o de desbloquear la información, en nuestro caso.

Cada sesión SSL contiene dos claves:

**1.** La clave pública es la usada para cifrar la información.

**2.** La clave privada es la usada para descifrar la información, de manera que vuelva a su estado original y sea legible.

- **El proceso**

Cada certificado SSL es otorgado para un servidor y página web específico por una entidad verificada por una Autoridad de Certificación. Cuando alguien usa su navegador para llegar a una página web con un certificado SSL, se produce un *handshake* (saludo inicial) entre el navegador y el servidor. Se solicita información sobre el servidor, la cual será visible en el navegador a través de un logo, icono o marca que valide el cifrado de la comunicación, como hemos comentado anteriormente. Si el usuario hace clic en dicho logo, se podrá observar información adicional como el periodo de validez

del certificado SSL, el dominio certificado, el tipo de certificado SSL y la Autoridad de Certificación que ha otorgado dicho certificado. Se establece, por tanto, una comunicación segura para esa sesión.

## 2.3. Estándares y tecnologías

En el siguiente apartado, definiremos los estándares y tecnologías disponibles para llevar a cabo el Proyecto Fin de Carrera. Enumeraremos las tecnologías basadas en comunicación por hardware.

### 2.3.1. Tecnologías basadas en software

Existen numerosas tecnologías que servirían para gestionar de forma remota los equipos de una empresa. Una muestra de las mismas pueden ser herramientas como Radmin Remote Control, BMC Track-it!, VNC Viewer, Webmin, LogMeIn Rescue, Kaseya Remote Access, NetSupport Manager Remote Control o más básicos como Telnet o SSH. Hay una extensa lista con características, versiones, sistemas operativos soportados, etc. en Wikipedia[1].

Como muestra de las características que pueden integrar las soluciones, a continuación mostramos una tabla con seis ejemplos comparadas de modo visual, reflejando algunos de los indicadores más relevantes:

| | Netviewer Support | Go To Assist | WebEx Remote Support | LogMe In Rescue | Show MyPC | Techinline Remote Desktop |
|---|---|---|---|---|---|---|
| Chat | Sí | Sí | Sí | Sí | Sí | Sí |
| Grabación de sesiones | Sí | Sí | Sí | Sí | Sí | Sí |
| Modo seguro | Sí | Sí | Sí | Sí | No | No |

[1] http://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software

| | | | | | | |
|---|---|---|---|---|---|---|
| Gestión de múltiples usuarios | Sí | Sí | Sí | Sí | Sí | No |
| No requiere instalación | Sí | Sí | Sí | Sí | Sí | Sí |
| Acceso remoto a Macs | Sí | Sí | Sí | Sí | Sí | Sí |
| Reinicio remoto de equipos | Sí | Sí | Sí | Sí | Sí | No |
| Transferencia de archivos | Sí | Sí | Sí | Sí | Sí | Sí |
| Invitación por e-mail | Sí | Sí | Sí | Sí | Sí | Sí |
| Estadísticas de uso | Sí | Sí | Sí | Sí | No | Sí |
| Pizarra | Sí | Sí | Sí | Sí | Sí | No |
| Recuperación de información del sistema | Sí | Sí | Sí | Sí | Sí | Sí |
| Soporte de múltiples monitores | Sí | Sí | Sí | Sí | Sí | Sí |
| Soporte de cámara web | Sí | Sí | Sí | No | No | No |
| Audio remoto | Sí | Sí | Sí | No | No | No |
| Multiple Monitor Support | Sí | Sí | Sí | Sí | No | No |
| Integración del logo coporativo en la interfaz | Sí | No | No | Sí | Sí | Sí |
| Número de sesiones simultáneas | 10 | 8 | 4 | 10 | 13 | 1 |
| Acceso a *smartphones* | No | No | No | Sí | No | No |
| Soporte desatendido | No | Sí | No | Sí | No | No |
| Cifrado SSL/TLS | Sí | Sí | Sí | Sí | Sí | Sí |

| | | | | | | |
|---|---|---|---|---|---|---|
| Número ID por cada sesión | Sí | Sí | Sí | Sí | Sí | Sí |
| Certificado VeriSign | Sí | Sí | Sí | Sí | No | No |
| Cifrado AES 128 bits | AES 256 bits | Sí | Sí | Sí | Sí | No |
| Email | Sí | Sí | Sí | Sí | Sí | Sí |
| FAQs | Sí | Sí | Sí | Sí | Sí | Sí |
| Soporte telefónico | Sí | Sí | Sí | Sí | Sí | Sí |
| Tutoriales | Sí | Sí | Sí | Sí | Sí | Sí |
| Foro de usuarios | Sí | No | No | Sí | No | No |
| Chat | No | No | Sí | No | Sí | No |
| **Requisitos del equipo cliente** | | | | | | |
| Windows 8 | Sí | No | No | No | No | Sí |
| Windows 7 | Sí | Sí | Sí | Sí | Sí | Sí |
| Windows Vista | Sí | Sí | Sí | Sí | Sí | Sí |
| Windows XP | Sí | Sí | Sí | Sí | Sí | Sí |

**Tabla 1. Comparativa de algunas soluciones software**[2]

La principal desventaja de todas estas soluciones es que se basan en comunicación por software, es decir, es necesario que el equipo cliente al que el administrador de TI se conecta esté encendido, con el sistema operativo funcionando y con el equipo escuchando las conexiones entrantes (es decir, la parte del servidor de la aplicación tiene que estar arrancado). Incluso, las soluciones comparadas en la tabla anterior, permiten el acceso remoto de usuarios mediante un enlace en el correo electrónico, lo que complica todavía más la solución. Este aspecto limita profundamente el número de casos en los que se podrá solucionar la incidencia, además de que, aunque permitiera apagar la flota de equipos de forma remota, imposibilita el volver a encenderlos para su mantenimiento o para cualquier otro fin.

Es por ello que será necesario recurrir a las pocas tecnologías que permiten comunicación por hardware, independientemente de que el equipo esté apagado o encendido, y de si en el momento de la conexión se encuentre dentro o fuera del sistema operativo. Esto permite mucha mayor flexibilidad e independencia del estado del equipo cliente.

[2] Fuente: http://remote-desktop-software-review.toptenreviews.com/

### 2.3.2. DASH (*Desktop and mobile Architecture for System Hardware*)

Se trata de un estándar abierto, creado por la *Desktop Management Task Force* (DMTF), que permite la gestión de sistemas a través de acceso remoto a bajo nivel. Esto incluye características como redirección a USB o dispositivos de almacenamiento, gestión remota de BIOS y KVM (*keyboard, video and mouse*).

Es una evolución del antiguo ASF (Alert Standard Format), que permitía la gestión remota, aunque muy limitada, desde el año 2001, con una nueva revisión en el 2003 y hasta el año 2007, cuando se publicó DASH v1.0.

Ofrece una gestión segura fuera de banda para PCs de escritorio y sistemas móviles en entornos empresariales distribuidos. Nace a partir de una colaboración entre las entidades pertenecientes a la DMTF con el objetivo de integrarla en sus plataformas para la administración remota segura, incluyendo la gestión fuera de banda de sistemas de escritorio y móviles de múltiples procesadores. Además de definir normas, han producido un SDK (*Software Development Kit* o Kit de Desarrollo de Software) de consola, una implementación de referencia y una suite de prueba de interoperabilidad – todos ellos compartidos como herramientas de código abierto.

DASH define un marco común para administrar clientes fuera de banda, lo que le da la flexibilidad para lograr tareas de administración esenciales, tales como control remoto de energía y arranque, parches, diagnóstico remoto, inventario de activos y seguridad en un ambiente empresarial distribuido, de múltiples vendedores.

DASH define normas abiertas basadas en servicios Web (WS-Management) para administrar equipos de escritorio, portátiles, servidores blade y *thin clients*.

#### Modelo de servicios

El modelo de servicios que usa DASH es el mismo que se implementa bajo la especificación SMASH (*Systems Management Architecture for Server Hardware*). SMASH es un conjunto de especificaciones formado por protocolos estándar para incrementar la productividad de la gestión de un centro de datos.

La gestión de un sistema que está dentro de banda se realiza con el soporte de componentes hardware que son utilizados por el sistema operativo del equipo a administrar, como, por ejemplo, su adaptador de red. La administración del equipo fuera de banda se realiza con recursos hardware y

componentes que son independientes del sistema operativo. Dichos recursos se dedican exclusivamente a la administración del sistema y permiten la gestión del hardware del sistema independiente del estado en el que éste se encuentre. Lo más normal es que estos recursos también estén disponibles cuando el sistema operativo está funcionando, como, por ejemplo, sería el caso de un procesador de servicio o un procesador de gestión de una placa base.

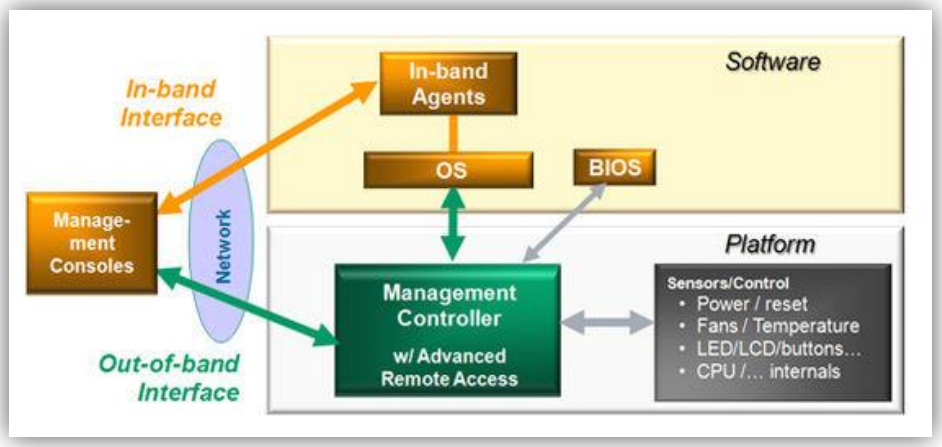



**Ilustración 3. Funcionamiento de DASH**

Unos ejemplos de fabricantes de hardware que implementan DASH en sus productos son:

- **Broadcom**, una de las principales marcas a nivel global en semiconductores para comunicaciones, fue la primera en proporcionar la tecnología a través de sus controladoras de red presentes en sus equipos OEM.

- **Marvell**, un fabricante de dispositivos de almacenamiento y de comunicaciones, entre otros, ofrece su controladora de red Yukon Gigabit Ethernet Controller con la tecnología DASH.

- **Realtek Semiconductor Corp**, un proveedor de semiconductores para redes de comunicaciones, periféricos de ordenadores y aplicaciones multimedia, también tiene integrado el soporte de DASH.

### 2.3.3. iAMT (*Intel Active Management Technology*)

La tecnología Intel AMT pertenece al conjunto de soluciones profesionales Intel vPro. Está basada en hardware y en firmware, y permite ciertas funcionalidades para el PC professional, como su gestión, mantenimiento, actualización y reparación. Intel AMT forma parte de Intel

*Management Engine*, el cual está integrado en todos los equipos con vPro. Éste está asociado a un procesador secundario localizado en la placa base. Intel AMT ha progresado añadiendo nuevas características a los estándares de la tecnología *DMTF Desktop and mobile Architecture for System Hardware (DASH)* y las versiones de AMT a partir de la 5.1 son implementaciones de las versiones 1.0/1.1 de DASH para la gestión fuera de banda.

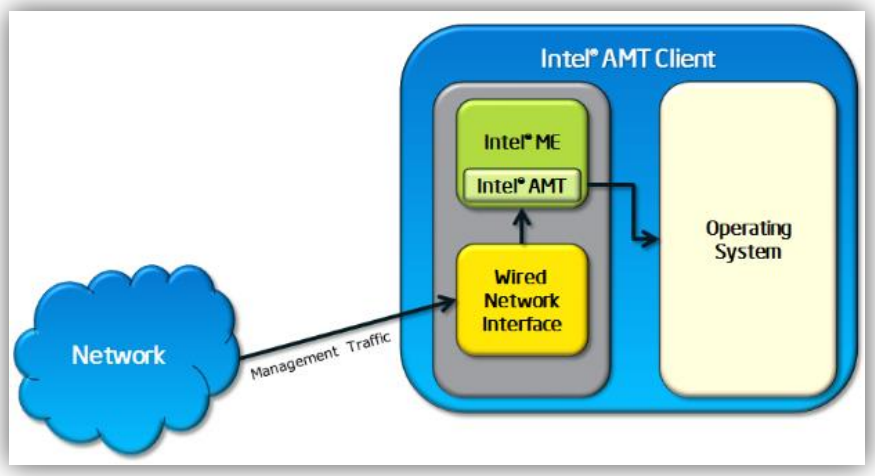



**Ilustración 4. Esquema simplificado de funcionamiento de iAMT**

AMT no está pensada para ser usada por sí sola, sino que necesita una aplicación de gestión para aprovechar todas sus características y funcionalidades. Esto le permite al administrador de TI el acceso al equipo con el fin de realizar tareas de forma remota y segura, que de otra manera podrían ser imposibles de realizar en un ordenador sin funciones de gestión remota integradas.

AMT incluye características de gestión remota basada en el hardware, seguridad, gestión de energía y configuración remota. Se basa en un canal de comunicación fuera de banda basado en el hardware que opera por debajo del sistema operativo, haciéndolo independiente de éste, ya esté en funcionamiento, ausente, corrupto o apagado. Este canal de comunicación también es independiente del estado del equipo, la presencia de un agente de gestión y el estado de distintos dispositivos hardware (como los discos duros, la placa base o la memoria RAM).

Muchas de las características de AMT están disponibles independientemente del estado del ordenador. Otras, en cambio, requieren que el equipo esté encendido (como la redirección a través de Serial over LAN –SoL- y el filtrado de tráfico de la red). Para ello, AMT tiene la capacidad de encender

el equipo de manera remota. Estas características basadas en el hardware se pueden combinar con *scripts* para automatizar el mantenimiento y el servicio, como por ejemplo a través de Windows PowerShell.

## 2.4. Evaluación comparativa

Para mostrar de forma rápida las diferencias fundamentales entre DASH 1.1 e iAMT 7.1, a continuación hay una tabla con algunas características comunes y no comunes entre ellos, para poder decidir la tecnología adecuada para solucionar el problema que plantea este proyecto:

| Característica | DASH v1.1 (Junio 2009) | iAMT 7.1 (Mayo 2011) |
|---|---|---|
| Control de arranque | Sí | Sí |
| Control de estado del sistema | Sí | Sí |
| Inventario hardware | Sí | Sí |
| Inventario software | Sí | Sí |
| Alerta de hardware | Sí | Sí |
| Serial Over LAN | Sí | Sí |
| NVRAM | Sí | Sí |
| Configuración remota | No | Sí |
| Filtros de defensa del sistema | No | Sí |
| Soporte de switch Keyboard/Video/Mouse (KVM) | Sí | Sí |
| Sujeto al hardware propietario de la marca | No | Sí |

**Tabla 2. Comparativa entre DASH 1.1 e iAMT 7.1**

Como comentario, añadir que las versiones comparadas son las disponibles en la fecha en que se realizó el trabajo de investigación. Además, DASH lleva sin ser actualizada desde junio de 2009. Actualmente hay una versión más reciente de AMT, la versión 8.0, pero la usada en el Proyecto es la revisión anterior.

La siguiente ilustración compara los pros y los contras de usar una tecnología propietaria de una marca, y otra de código libre (vPro y DASH, respectivamente):

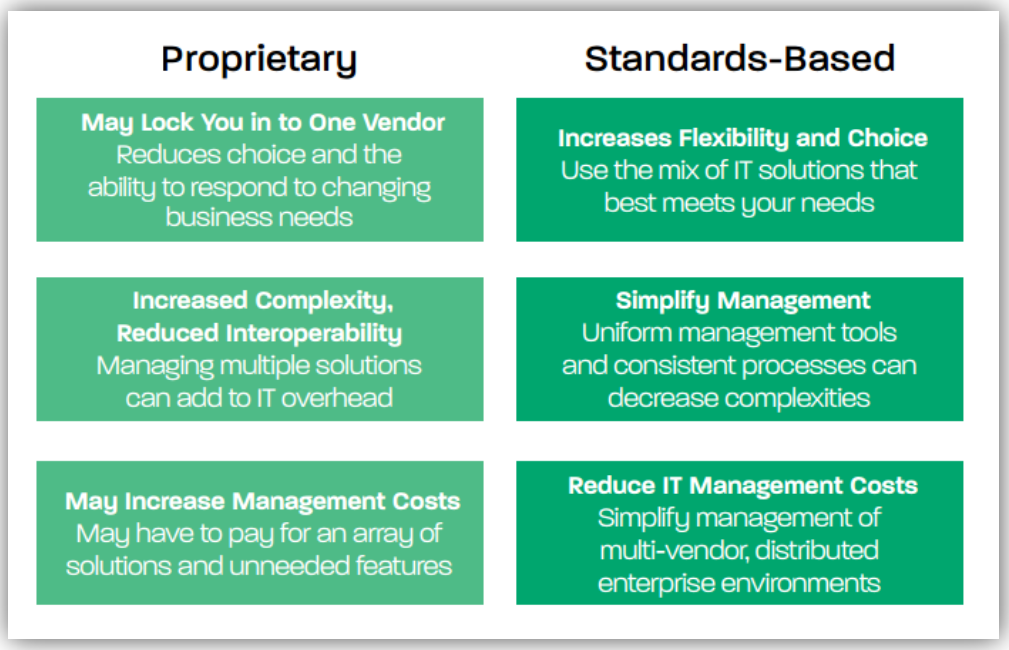



**Ilustración 5. Comparativa entre tecnología propietaria y de código libre**

## 2.5. Conclusiones

A pesar de las ventajas que se observan en la tabla anterior acerca de escoger DASH, como no estar sujeto a un hardware específico para poder emplearla, las diferencias de funcionalidad y el soporte que ofrecen los impulsores de ambas tecnologías (recordemos que DASH 1.1 se actualizó por última vez en junio de 2009), son motivos suficientes para decantarnos por la solución de gestión remota de Intel.

Es por ello que utilizaremos vPro para obtener acceso remoto completo al equipo cliente, y más concretamente implantaremos un entorno *Fast Call For Help* (a partir de ahora nos referiremos a esta tecnología por las siglas FCFH), que se basa en iAMT y además añade la ventaja de que es el propio cliente el que solicita la asistencia remota, facilitando el establecimiento de la comunicación entre la consola de gestión y el cliente.

# **Capítulo 3.** Análisis y diseño de la solución

A continuación se describirán de manera formal todos los elementos del entorno, describiéndolos uno a uno y determinando qué función tendrán y qué valor aportarán al conjunto de la solución.

Cada componente tiene unos requisitos que el sistema debe cumplir, por lo que también enumeraremos aquellas características que se deben cumplir para que la solución funcione correctamente y sin inestabilidades.

A modo introductorio, comenzaremos describiendo de qué partes consiste un entorno *Fast Call For Help* y después la analizaremos en detalle.

La tecnología consta de:

- Un equipo cliente, que será quien emita la solicitud de asistencia remota.
- Una zona desmilitarizada, que actuará como zona intermedia entre el equipo cliente y la consola y será donde se sitúe la puerta de enlace para recibir las solicitudes de asistencia.
- Un equipo consola, que se encargará de responder a la solicitud de ayuda conectándose al equipo cliente que la emitido.

## 3.1. Solución propuesta

### 3.1.1. ¿En qué consiste?

*Fast Call For Help*, antes conocida como CIRA (*Client-Initiated Remote Access*) o CILA (*Client-Initiated Local Access*), es una tecnología de gestión remota que hace uso de iAMT. Es por ello que será necesario que el equipo gestionado esté equipado con la tecnología Intel vPro. Esta tecnología está especialmente pensada para entornos en los que el ordenador cliente se encuentra fuera de la red corporativa, y no está localizable directamente a través de la consola por encontrarse tras un *router* con funcionalidad NAT, y por lo tanto, con una IP pública para varios equipos.

*Fast Call For Help* permite al equipo cliente establecer una llamada al equipo consola para solicitar ayuda al administrador de TI por una avería o incidencia en su equipo, esté donde esté.

La solicitud de ayuda, previamente configurada en el equipo cliente con los parámetros necesarios para establecer la conexión con el servidor Apache localizado en la red interna de la empresa, se puede emitir tanto estando dentro del sistema operativo como fuera. Este mecanismo permite mayor flexibilidad a la hora de diagnosticar y/o reparar averías, ya que puede que ni siquiera el sistema operativo residente arranque y el usuario podrá, aún así, solicitar ayuda para reinstalar una imagen limpia del mismo u otro sistema operativo, reparar ficheros dañados, realizar un escaneo con antivirus, *tests* de memoria, pruebas de detección de sectores defectuosos en el disco duro, etc.

Por lo tanto, lo único que será necesario para establecer una conexión es que el cliente se encuentre dentro del ámbito corporativo y que el administrador de TI inicie una conexión, ya que tendrá localizado al cliente mediante nombre de host, dirección IP, etc. o si se encuentra fuera de éste, que el usuario solicite asistencia mediante un botón dentro de Windows, o con una combinación de teclas si está fuera del sistema operativo.

El entorno de *Fast Call For Help* se compone de tres partes claramente diferenciadas, tal y como se muestra en la siguiente ilustración: parte de la consola de gestión (dentro de la red coporativa), DMZ y parte de cliente (fuera de la red corporativa).

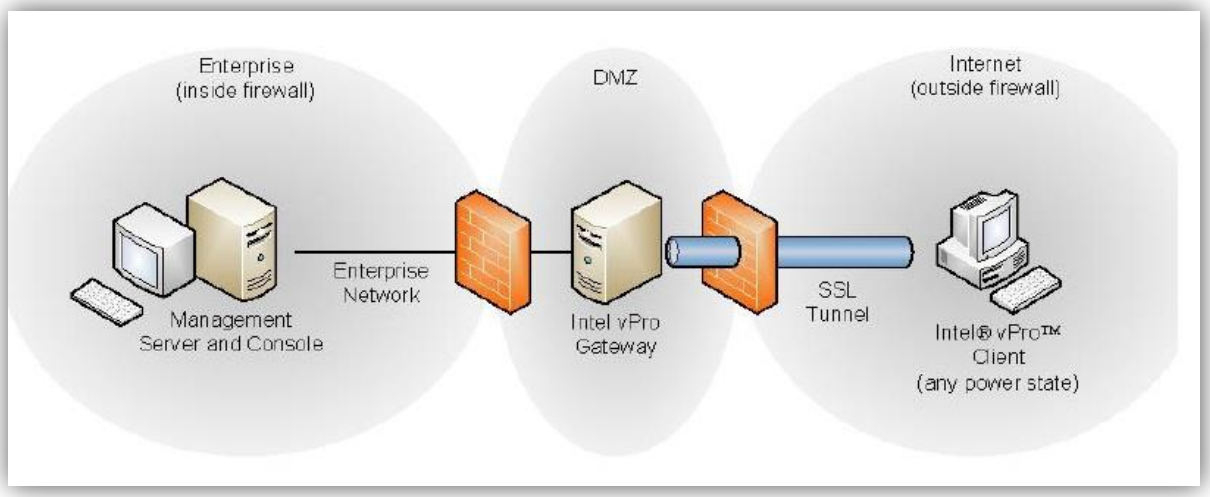



**Ilustración 6. Esquema de entorno FCFH**

### 3.1.2. Equipo cliente

Debe ser un ordenador con la tecnología vPro integrada, ya que será la que permitirá iniciar la solicitud de ayuda a través de iAMT y su *Management Engine*, y permitir la conexión de la consola de gestión contra el equipo cuando sea necesario. Como he comentado antes, puede estar conectado por cable a la red, o de manera inalámbrica.


**Ilustración 7. Simbolización de equipo con vPro**

### 3.1.3. DMZ (*Demilitarized Zone* o Zona Desmilitarizada)

Se trata de una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa.

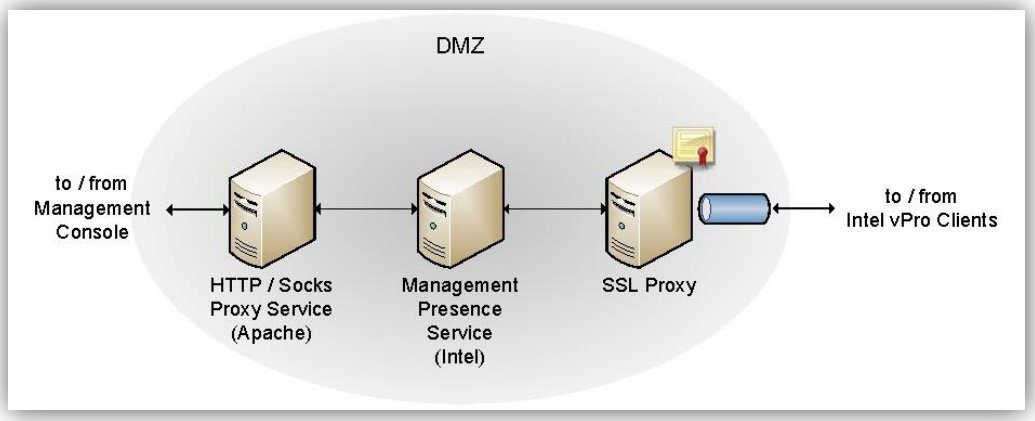



**Ilustración 8. Componentes de la DMZ**

Los equipos ubicados en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada.

### 3.1.4. Consola de gestión

Será la que manejará el administrador de TI para poder tratar la incidencia del cliente. Se podrá situar tanto dentro como fuera del entorno empresarial, porque siempre estará conectado a la IP del MPS a través del software de gestión.

## 3.2. Requisitos

Los requisitos del entorno se especifican en una plantilla de referencia, cuya disposición es la siguiente:

| Identificador | RX-YY |
|---|---|
| **Elemento** | |
| **Descripción** | |
| **Carácter** | |

Tabla 3. RX-YY. Plantilla de requisitos

El "Identificador" de la tabla representa qué tipo de requisito es el que se desglosa. El campo identificado por la letra X representará mediante la letra "S" si el requisito es de software, "H" si es de hardware, "F" si es de funcionalidad o "R" si es de restricción. Las letras "YY" representarán un número de dos dígitos, partiendo del 01 e incrementando en una unidad por cada requisito que se enumere.

En el campo "Elemento" se define cuál de los componentes es el afectado por el requisito, es decir, "DMZ", "Cliente" o "Consola". A su vez, "DMZ" puede referirse a sus tres componentes: "Stunnel", "Apache" o "MPS".

En el campo "Descripción" se ofrece un comentario detallado del requisito.

El campo "Carácter" determina si el requisito es "Obligatorio" u "Opcional". Si fuera "Opcional", quiere decir que el requisito es el recomendado pero se pueden recurrir a otras soluciones, aunque no se aseguraría el correcto funcionamiento del entorno.

El siguiente campo, "Fuente", indica el origen del requisito. Si fue determinado por el cliente, tendrá el valor "Cliente", y si fue concretado por el analista, tomará este otro valor.

Por último, el elemento "Prioridad" indica el grado de urgencia de aplicación del requisito para el proyecto.

| Identificador | RF-01 |
|---|---|
| **Elemento** | Sistema |
| **Descripción** | Se debe permitir una gestión remota de los equipos cliente. |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

Tabla 4. RF-01. Gestión remota

| Identificador | RF-02 |
|---|---|
| **Elemento** | Sistema |
| **Descripción** | El entorno de acción será tanto dentro de la red corporativa como fuera de ella. |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 5. RF-02. Gestión dentro y fuera de la red corporativa**

| Identificador | RF-03 |
|---|---|
| **Elemento** | Sistema |
| **Descripción** | La solución debe permitir la gestión remota pese a errores del sistema operativo (fuera de banda). |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 6. RF-03. Gestión dentro y fuera de banda**

| Identificador | RF-04 |
|---|---|
| **Elemento** | Sistema |
| **Descripción** | La gestión remota será bidireccional. Puede ser tanto iniciada por el usuario como por el asistente o administrador de IT. |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 7. RF-04. Gestión bidireccional**

| Identificador | RF-05 |
|---|---|
| **Elemento** | Sistema |
| **Descripción** | El sistema permitirá la resolución de incidencias de forma desasistida por parte del usuario. |
| **Carácter** | Opcional |
| **Fuente** | Cliente |
| **Prioridad** | Media |

**Tabla 8. RF-05. Gestión desasistida por el usuario**

| Identificador | RF-06 |
|---|---|
| **Elemento** | Sistema |
| **Descripción** | Se podrá atender tanto a tareas de resolución de incidencias como de mantenimiento del equipo cliente. |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 9. RF-06. Gestión de incidencias y mantenimiento**

| Identificador | RF-07 |
|---|---|
| **Elemento** | Equipo cliente |
| **Descripción** | Los equipos a gestionar necesitarán una configuración previa dentro de la red corporativa para poder ser atendidos una vez fuera. |
| **Carácter** | Obligatorio |
| **Fuente** | Analista |
| **Prioridad** | Alta |

**Tabla 10. RF-07. Configuración previa de los equipos**

| Identificador | RS-01 |
|---|---|
| **Elemento** | Equipo cliente |
| **Descripción** | Actualizar los controladores de iAMT, también llamados controladores MEI (*Management Engine Interface*). Si el equipo viene plataformado con sistema operativo, ya vienen integrados en él, aunque puede que con una versión anterior a la última disponible. |
| **Carácter** | Opcional |
| **Fuente** | Analista |
| **Prioridad** | Media |

**Tabla 11. RS-01. Actualizar controladores iAMT**

| Identificador | RS-02 |
|---|---|
| **Elemento** | Equipo cliente |
| **Descripción** | Si la conexión es inalámbrica, el cifrado debe ser de tipo WPA-PSK. |
| **Carácter** | Obligatorio |
| **Fuente** | Analista |
| **Prioridad** | Alta |

**Tabla 12. RS-02. Cifrado de conexión inalámbrica**

| Identificador | RS-03 |
|---|---|
| **Elemento** | Equipo cliente |
| **Descripción** | ***Management Engine*** debe estar configurado (provisionado). Para ello será necesario configurar los parámetros de esta tecnología en la interfaz MEBx. Esto se puede hacer, o bien antes de entregarle el equipo al usuario y que empiece a funcionar con él, o bien a posteriori. No afectará al uso del mismo durante las tareas diarias del usuario. |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 13. RS-03. ME debe estar provisionado**

| Identificador | RS-04 |
|---|---|
| **Elemento** | DMZ (MPS) |
| **Descripción** | Versión de *Management Presence Server*: 1.2.0.21. Es la versión utilizada en el Proyecto, pero puede que haya versiones actuales con más funcionalidades y mayor compatibilidad. |
| **Carácter** | Opcional |
| **Fuente** | Cliente |
| **Prioridad** | Media |

**Tabla 14. RS-04. Versión de MPS**

| Identificador | RS-05 |
|---|---|
| **Elemento** | DMZ (MPS) |
| **Descripción** | Sistema operativo: Windows Server 2008 R2 Standard (64 bits). También se puede implementar en una máquina con Windows Server 2003. |
| **Carácter** | Opcional |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 15. RS-05. Sistema operativo MPS**

| Identificador | RS-06 |
|---|---|
| **Elemento** | DMZ (Apache) |
| **Descripción** | Versión del servidor HTTP Apache: 2.2.8. Es la versión utilizada en el Proyecto, pero puede que haya versiones actuales con más funcionalidades y mayor compatibilidad. |
| **Carácter** | Opcional |
| **Fuente** | Cliente |
| **Prioridad** | Media |

**Tabla 16. RS-06. Versión de Apache**

| Identificador | RS-07 |
|---|---|
| **Elemento** | DMZ (Stunnel) |
| **Descripción** | Versión Stunnel: 4.31. Es la versión utilizada en el Proyecto, pero puede que haya versiones actuales con más funcionalidades y mayor compatibilidad. |
| **Carácter** | Opcional |
| **Fuente** | Cliente |
| **Prioridad** | Media |

**Tabla 17. RS-07. Versión de Stunnel**

| Identificador | RS-08 |
|---|---|
| **Elemento** | Consola |
| **Descripción** | Sistema operativo Windows de 32 bits. Instalarlo en Sistemas Operativos de 64 bits provocará incompatibilidades en *Manageability Commander Tool*. |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 18. RS-08. Sistema operativo consola**

| Identificador | RS-09 |
|---|---|
| **Elemento** | Consola |
| **Descripción** | Instalación de Microsoft .NET Framework 2.0 |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 19. RS-09. Instalación de Microsoft .NET Framework 2.0**

| Identificador | RH-01 |
|---|---|
| **Elemento** | Equipo cliente |
| **Descripción** | El equipo debe tener integrada la tecnología Intel vPro (todos los equipos que disponen de ella llevan un pequeño adhesivo identificativo visible). Éste está presente en los equipos que integran, entre otros, los siguientes *chipsets*: Intel 965, Q35, Q945 Express, GM965 y Series 4 Express. |
| **Carácter** | Obligatorio |
| **Fuente** | Cliente |
| **Prioridad** | Alta |

**Tabla 20. RH-01. Cliente con vPro**

| Identificador | RH-02 |
|---|---|
| **Elemento** | DMZ |
| **Descripción** | Instalar los tres componentes (MPS, Stunnel y Apache) en la misma máquina. Se pueden instalar en equipos distintos, pero deberán tener conexión entre ellas. |
| **Carácter** | Opcional |
| **Fuente** | Analista |
| **Prioridad** | Baja |

**Tabla 21. RH-02. Instalación de los componentes de la DMZ**

| Identificador | RH-03 |
|---|---|
| **Elemento** | Consola |
| **Descripción** | Versión mínima de firmware de iAMT: 4.0. También funcionará en máquinas que tengan versiones 1.0 – 3.X pero con algunas limitaciones. |
| **Carácter** | Opcional |
| **Fuente** | Analista |
| **Prioridad** | Alta |

**Tabla 22. RH-03. Versión mínima de firmware de iAMT**

| Identificador | RH-04 |
|---|---|
| **Elemento** | DMZ (Apache) |
| **Descripción** | Conexión a Internet o, de forma local, a la consola de gestión para dirigir el tráfico de las llamadas de los clientes. |
| **Carácter** | Obligatorio |
| **Fuente** | Analista |
| **Prioridad** | Alta |

**Tabla 23. RH-04. Conectividad de Apache**

| Identificador | RH-05 |
|---|---|
| **Elemento** | DMZ (Stunnel) |
| **Descripción** | Conexión a Internet para escuchar las llamadas de los clientes que soliciten asistencia. |
| **Carácter** | Obligatorio |
| **Fuente** | Analista |
| **Prioridad** | Alta |

**Tabla 24. RH-05. Conectividad de Stunnel**

| Identificador | RH-06 |
|---|---|
| **Elemento** | Consola |
| **Descripción** | Requisitos mínimos de hardware para que funcione correctamente *Manageability Commander Tool*:<br>• 1 GB RAM.<br>• 5 GB de espacio libre en el disco duro.<br>• Conexión Ethernet 100 MB. |
| **Carácter** | Obligatorio |
| **Fuente** | Analista |
| **Prioridad** | Alta |

**Tabla 25. RH-06. Requisitos hardware mínimos de la consola**

| Identificador | RR-01 |
|---|---|
| **Elemento** | Equipo cliente |
| **Descripción** | El equipo debe tener conexión a la red eléctrica. Esto se debe a dos razones: la primera es la seguridad, y la segunda es la practicidad. Con la primera se evitará tener conexiones indeseadas si se tratara de un equipo portátil y el usuario se encontrara transportándolo, o simplemente si no lo estuviera utilizando. Con la segunda se evita un desgaste adicional de la batería que interrumpiera inesperadamente la conexión remota. |
| **Carácter** | Obligatorio |
| **Fuente** | Analista |
| **Prioridad** | Alta |

**Tabla 26. RR-01. Conexión a la red eléctrica**

Como parte de los requisitos, se presenta una tabla en la siguiente página que muestra algunas de las funcionalidades elementales de AMT, entre ellas *Fast Call For Help*, y la versión mínima de AMT que se requiere para que funcione cada una de ellas.

| *Caracte-rística / Versión* | AMT 1.0 (Desktop) | AMT 2.0/2.1 (Desktop) | AMT 2.5/2.6 (Mobile) | AMT 3.0 (Desktop) | AMT 4.0 (Mobile) | AMT 5.0 (Desktop) | AMT 6.0 (Desktop & Mobile) | AMT 7.0 & 8.0 (Desktop & Mobile) |
|---|---|---|---|---|---|---|---|---|
| **Inventario hardware** | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **Encendido /apagado remoto** | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **SOL/IDER** | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **Gestor de eventos** | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **Almacena-miento de información de terceros** | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **Servidor web** | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **HTTP Digest/TLS** | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **Políticas de energía** | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| **Configuración remota** | No | 2.2 y siguientes | 2.6 y siguientes | Sí | Sí | Sí | Sí | Sí |
| **Configuración inalámbrica** | No | No | Sí | No | Sí | No | Sí | Sí |
| **Detección de entorno** | No | No | Sí | No | Sí | No | Sí | Sí |
| **Fast Call For Help** | No | No | No | No | Sí | Sí | Sí | Sí |

**Tabla 27. Funcionalidades y versiones mínimas de AMT[3]**

[3] Versión reducida de la tabla disponible en: http://en.wikipedia.org/wiki/Intel_AMT_versions

Seguidamente, procederemos a describir el diseño arquitectónico del sistema. La información recogida a continuación servirá de guía para la implementación de la aplicación.

## 3.3. Diseño del sistema

En esta sección abordaremos la definición de cada una de las partes que conforman el entorno presentado en este Proyecto Fin de Carrera.

### 3.3.1. Equipo cliente con vPro

La configuración de red del equipo puede hacerse a través de las consolas de gestión, o bien mediante distintos métodos de configuración automática o manual que se ofrecen. La forma más básica que existe es entrar en la MEBx (*Management Engine BIOS extension*, una herramienta con interfaz gráfica fuera del sistema operativo para configurar iAMT) y establecer los parámetros manualmente. Todas las formas de configuración tienen en común que deberán determinar si la dirección IP del equipo será estática o dinámica, su máscara de subred, el servidor DHCP en su caso, el dominio al que perteneciera, su identificación dentro del dominio y la puerta de enlace. El proceso de configuración es muy elemental, pero para este proyecto he utilizado el método de HBP (*Host Based Provisioning*), que permite establecer los parámetros de iAMT a través de un programa en Windows.

Esta configuración, también llamada "provisionamiento", se puede hacer tanto si el usuario ya se encuentra utilizando el equipo, como si todavía no ha comenzado a trabajar con él. La configuración *a posteriori* no afecta al funcionamiento del equipo, ya que los parámetros establecidos no interfieren con la configuración de conexión del equipo a la red a la que estuviera conectado para acceder a Internet. Como hemos dicho, el *Management Engine* es un elemento independiente del sistema operativo.

Los parámetros internos del MEBx (tales como IP, puerta de enlace, máscara de subred, etc.) no tienen por qué coincidir con los parámetros de configuración de la tarjeta de red en el sistema operativo. En versiones anteriores de vPro esto no era así, lo que provocaba muchos fallos e incompatibilidades, pero al corregirlo se ha conseguido más comodidad y funcionalidad a la hora de establecer una solicitud de asistencia.

### 3.3.2. DMZ

El conjunto de los componentes que la forman se denomina *vPro Enabled Gateway* (o VPEG) y como su propio nombre indica, servirá de plataforma de comunicación entre los clientes con tecnología vPro y la consola de gestión.

Se divide, por lo tanto, en tres partes claramente diferenciadas: por un lado se situará el MPS (*Management Presence Server*, también llamado *Intel vPro Gateway*); por otro lado, el servidor encargado de gestionar todo el tráfico HTTP (Apache) y por último, el Stunnel, que será quien establezca el canal cifrado entre el cliente y la DMZ para garantizar una conexión segura.

- El MPS permite gestionar las llamadas de los equipos profesionales que se encuentran fuera de la red corporativa. Se encuentra disponible en el SDK (*Software Development Kit* o Kit de Desarrollo de Software) de Intel AMT y como tal, se ofrece de manera gratuita pero no soportada. Está pensado para un uso básico de *Fast Call For Help* y para que empresas desarrolladoras de software lo tomen como base para crear su propio *gateway* y comercializarlo.

  El MPS se encargará de mediar entre la consola de gestión y los equipos fuera de la red corporativa. Será responsable del tráfico SOAP. Se deberá ubicar en el servidor de la empresa que desee gestionar los equipos fuera de su red.

- El servidor HTTP Apache es necesario para actuar de proxy HTTP/Socks entre la consola de gestión y el MPS. Es responsable de todo el tráfico HTTP, que en términos de los servicios de AMT son todos los comandos excepto la redirección y la capacidad KVM, que veremos más adelante.
- Stunnel es el software que establecerá un túnel seguro entre la DMZ y el cliente vPro que solicita la asistencia.

### 3.3.3. Consola de gestión

Para este proyecto hemos utilizado la consola gratuita de Intel, *Manageability Commander Tool*, incluida dentro del conjunto de herramientas de libre disposición *Manageability Developer Toolkit* v6.0.10314. En ella se registrarán los equipos que soliciten el servicio de FCFH y se podrá conectar a ellos a través de KVM o SoL para solucionar la incidencia de la manera que más se adecue a la ocasión.

Como comentaremos posteriormente, y tal y como hemos detallado en el **Apéndice II**, se pueden utilizar otras consolas de pago más complejas y con más funcionalidad que el software gratuito proporcionado por Intel. Sin embargo,

este Proyecto Fin de Carrera empleó esta solución por ser la más accesible y sencilla de utilizar, además de ser suficiente para el entorno que íbamos a implantar. En un escenario con muchos equipos que pudieran solicitar asistencia, se podría emplear otra infraestructura más compleja, que incluyera un servidor DHCP, DNS, Active Directory, etc., a pesar del incremento en el presupuesto final del proyecto.

## 3.4. Esquema de funcionamiento:

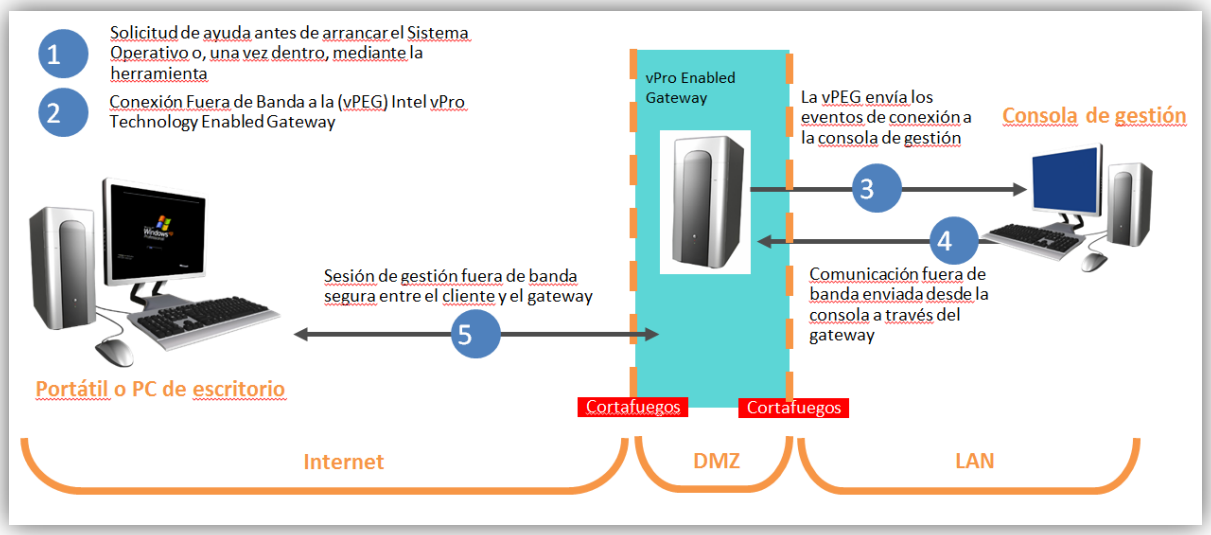



**Ilustración 9. Esquema de funcionamiento de FCFH**

1 El usuario, localizado en cualquier sitio fuera del ámbito corporativo y con acceso a Internet, presiona la combinación de teclas predefinida para solicitar la ayuda a la consola de gestión.

2 Se establece una conexión fuera de banda a la vPEG (vPro Enabled Gateway, o puerta de enlace) localizada dentro de la zona desmilitarizada, a su vez dentro del ámbito corporativo.

3 La puerta de enlace recibe la solicitud de ayuda a través de un túnel seguro y envía los datos de la solicitud a la consola de gestión.

4 La consola de gestión responde a la llamada y se conecta de nuevo con la puerta de enlace para establecer una sesión de asistencia remota. Enruta WS-MAN SOAP y los comandos de redirección de vuelta a la puerta de enlace.

5 La vPEG crea un túnel proxy usando SSL para establecer un canal de comunicación seguro entre la consola de gestión y el cliente. El administrador de TI ya puede operar remotamente con el equipo que solicitó la ayuda.

# **Capítulo 4.** Implantación

En este capítulo mostraremos cómo instalar y configurar toda la plataforma *Fast Call For Help* para crear un entorno que permita a una empresa ofrecer asistencia remota a sus empleados.

Antes de llevar a cabo todas las instalaciones y configuraciones, habrá que hacer una serie de modificaciones en el sistema y en el cortafuegos de Windows Server. Por un lado, hay que configurar la interfaz de red deshabilitando todos los servicios y protocolos de red excepto TCP/IP. También hay que deshabilitar el registro de direcciones en DNS, y deshabilitar NetBIOS sobre TCP/IP. Además, crearemos unas reglas de entrada y salida para los puertos que posteriormente necesitaremos configurar en las aplicaciones. Esto es necesario para garantizar que el tráfico que llegue a los puertos anteriormente descritos no se filtrará y descartará:

- Usando *Seguridad Avanzada de Windows Firewall*, creamos una regla para permitir todo el tráfico entrante desde cualquier puerto a los puertos locales 443, 8080, 8090 y 7793.
- En la misma aplicación, creamos una regla para permitir todo el tráfico saliente desde cualquier puerto de nuestro equipo a cualquier puerto remoto.

Hay que tener en cuenta las reglas que he aplicado en este caso son para este entorno limitado en cuanto a infraestructura y clientes vPro. Las empresas tienen sus propias medidas de seguridad para mantener seguros sus servidores en la red interna.

Para comenzar con el proceso de instalación y configuración, comenzaré dividiendo el entorno en sus tres partes claramente diferenciadas y explicando el procedimiento en cada uno de ellos.

## 4.1. DMZ

La configuración y los componentes del entorno serán los siguientes:

- Sistema operativo: Windows Server 2008 R2 Standard (64 bits)
- Interfaz de red: Única interfaz de red con IP estática
- Proxy SSL: Stunnel 4.31
- Proxy HTTP / Socks: Apache 2.2.8 con módulos proxy de Intel
- Management Presence Server: Intel MPS sin modificar
- Dirección IP por defecto: 80.27.69.15 (configurable)
- Puertos de red por defecto: 443, 8080, 8090 y 7793 (configurables)

En esta parte tendremos que configurar a su vez, por separado (aunque en la misma máquina), los tres componentes de la DMZ: Stunnel, MPS y servidor Apache.

### 4.1.1. Stunnel y certificados

Instalamos el software Stunnel con la configuración por defecto. A continuación instalamos los certificados para poder crear el túnel seguro entre el cliente y la DMZ.

Será necesario un certificado que incluya la autentificación del servidor para la acreditación del proxy SSL. Este certificado se enviará al equipo cliente con vPro y será utilizado para comprobar que se están comunicando a través de un túnel de comunicación seguro. El certificado del servidor y todos los demás certificados en la cadena firmante podrán tener un cifrado de 1024 a 2048 bits. Estos certificados fueron creados por nosotros expresamente con el propósito de desarrollar el Proyecto, pero para un entorno profesional como éste se podría recurrir a la herramienta gratuita de gestión de certificados "XCA: X Certificate and key management", generarlos con OpenSSL o incluso crearlos con la Autoridad de Certificación que viene integrada en el sistema operativo Windows Server 2008 (el cual está instalado en el equipo que usaremos como *gateway*). El uso de estos certificados será privado, por lo que no es necesario que los firme una AC real. Simplemente se usarán para verificar que la conexión se hace contra el servidor que previamente habíamos configurado, y no uno desconocido.

Para una correcta implantación de este Proyecto Fin de Carrera dispondremos de los siguientes certificados:

- *ServerCertificateKey.pem*: contendrá el certificado del servidor MPS y la clave privada asociada al mismo, la cual tendrá una longitud de 2048 bits y será cifrada mediante RSA.

- *ServerCertificate.pem*: incluirá el certificado del servidor MPS. Será el que se envíe al cliente cuando se establezca una conexión para que éste verifique que es el servidor correcto.

- *ClientCertificateSigningChain.pem*: contendrá el certificado raíz, cada uno de los certificados intermedios y por último el certificado de la Autoridad de Certificación. Servirá para que el cliente se autentifique a la hora de crear el túnel seguro. En nuestro caso no hemos usado ningún certificado intermedio, y tampoco hemos empleado la verificación del cliente mediante certificado, sino que utilizamos una autenticación mediante nombre de usuario y contraseña, pero para un entorno empresarial el certificado del cliente sería una alternativa a considerar.

- vProLab Offline Root CA 2048 es el certificado raíz que tendrán instalado los clientes para verificar que el servidor de provisionamiento es un servidor confiable.

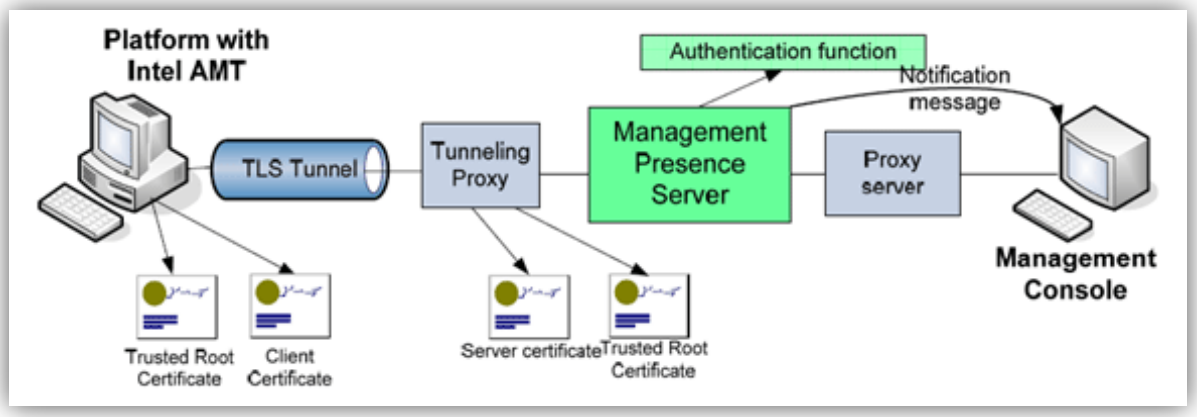



**Ilustración 10. Esquema de entorno FCFH**

Después de copiar los certificados al directorio de instalación de Stunnel, hay que definirlo como un servicio del sistema operativo mediante una opción del propio software. Por último, hay que hacer que dicho servicio arranque cuando el servicio de Windows "TCP/IP" se inicie, creando una entrada en el registro, en la ruta *HKLM\SYSTEM\CurrentControlSet\services\stunnel*.

El siguiente paso es configurar la interfaz de red y el puerto de salida a Internet. Éste será el encargado de escuchar las solicitudes de asistencia de los clientes. Todo el tráfico enviado entre el cliente vPro y esta dirección IP estará cifrada usando SSL. El puerto configurado es el 443.

Después hay que modificar la IP de la interfaz de red, la máscara de subred y la puerta de enlace en el fichero de configuración de Stunnel.

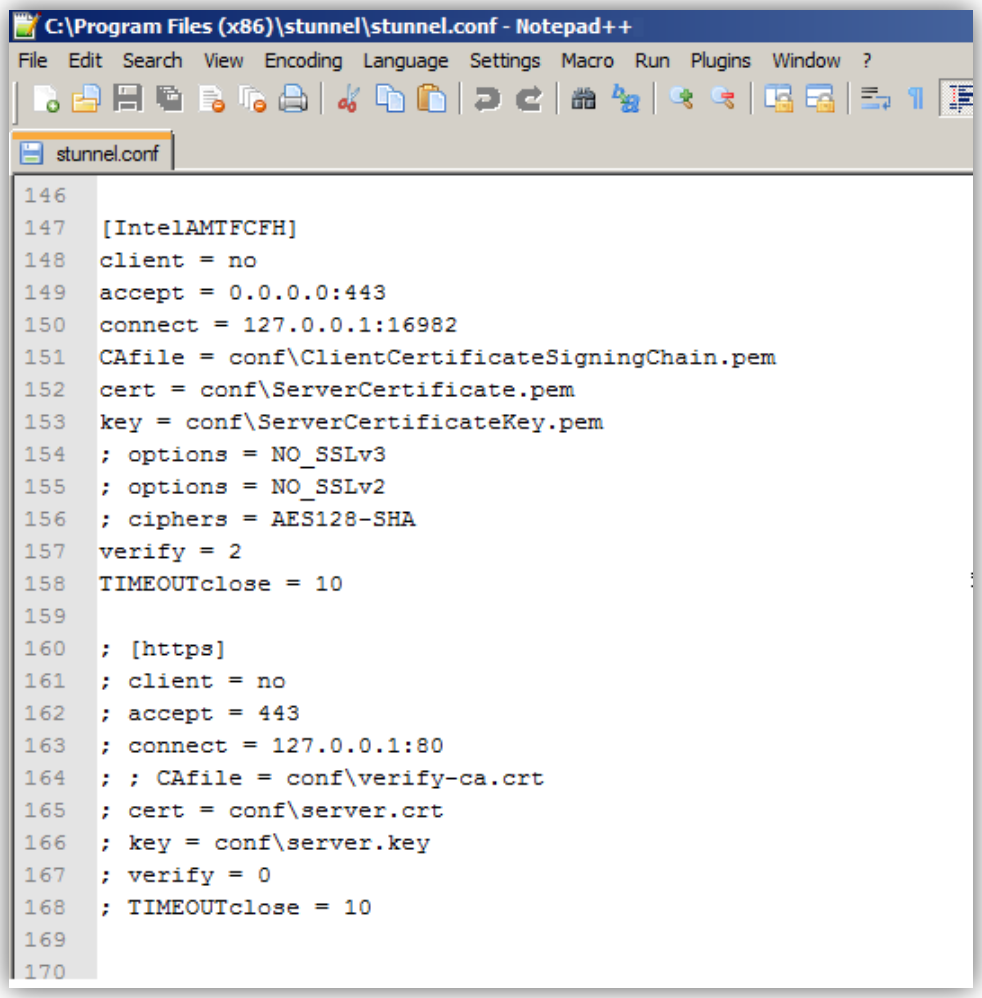



**Ilustración 11. Configuración de Stunnel**

### 4.1.2. MPS

Una vez instalado el software MPS, procedemos a instalar el paquete de Microsoft Visual C++ 2005 SP1, que será necesario para el correcto funcionamiento del MPS.

Después, cambiaremos en el fichero de configuración de MPS la dirección IP y el puerto que usará el proxy SSL (Stunnel) para redirigir las solicitudes de conexión de los clientes vPro al MPS. Al encontrarse Stunnel y MPS instalados en la misma máquina y por lo tanto tener la misma dirección IP, utilizaremos la de *loopback*, es decir, 127.0.0.1. El puerto usado para esta labor es el 16982.

### 4.1.3. Servidor HTTP/Socks Apache

Instalamos el software con la configuración por defecto. Para establecer los parámetros de configuración manualmente, es necesario detener el servicio Apache, que se inicia por defecto después de la instalación.

Copiamos los módulos de Intel incluidos en el software MPS dentro de las carpetas de instalación de Apache. Después, copiamos también el fichero de configuración (*HTTPD.conf*) en la carpeta con el mismo fichero de Apache.

El siguiente paso es configurar el puerto y la dirección IP en el lado de la Intranet, con conexión directa al proxy HTTP (Apache) desde la consola de gestión. Esta dirección será la usada por Apache para escuchar las solicitudes de conexión a través de la Intranet desde la consola del administrador de TI usando HTTP para comunicarse con los clientes vPro. La dirección IP será una privada, asignada previamente por el administrador de red. En este caso, usaremos la 192.168.1.21, y el puerto fue el 8080.

Ahora hay que configurar el puerto y la dirección IP en la Intranet con conexión directa al proxy Socks (Apache) desde la consola de gestión. Esta dirección será la usada por Apache para escuchar las solicitudes entrantes a través de la Intranet usando el protocolo de redirección para comunicarse con los clientes vPro. En este caso, la dirección IP es la misma que la del servidor HTTP: 192.168.1.21, y el puerto es el 8090.

Por último, hay que configurar la interfaz del MPS que usará para escuchar conexiones entrantes desde la consola de gestión para conectarse al servidor usando el protocolo SOAP. La dirección IP es la misma que en los dos casos anteriores, 192.168.1.21, y el puerto es el 7793.

## 4.2. Despliegue del cliente

Partiendo de que contamos con que el equipo cumple con los requisitos de hardware y software mencionados anteriormente, el primer paso para configurar el equipo cliente es provisionarlo con la configuración necesaria para que pueda localizar el MPS y comunicarse con él cuando se encuentre fuera del entorno corporativo.

Hay varios modos de provisionamiento, en función del entorno en el que nos encontremos. Como en nuestro caso sólo desplegaremos un cliente, lo haremos de forma manual. El resto de los modos de provisionamiento están comparados en el glosario. Utilizaremos el software **ACU Wizard** para establecer todos los parámetros necesarios, como el nombre del MPS, el certificado raíz, los puertos, etc.

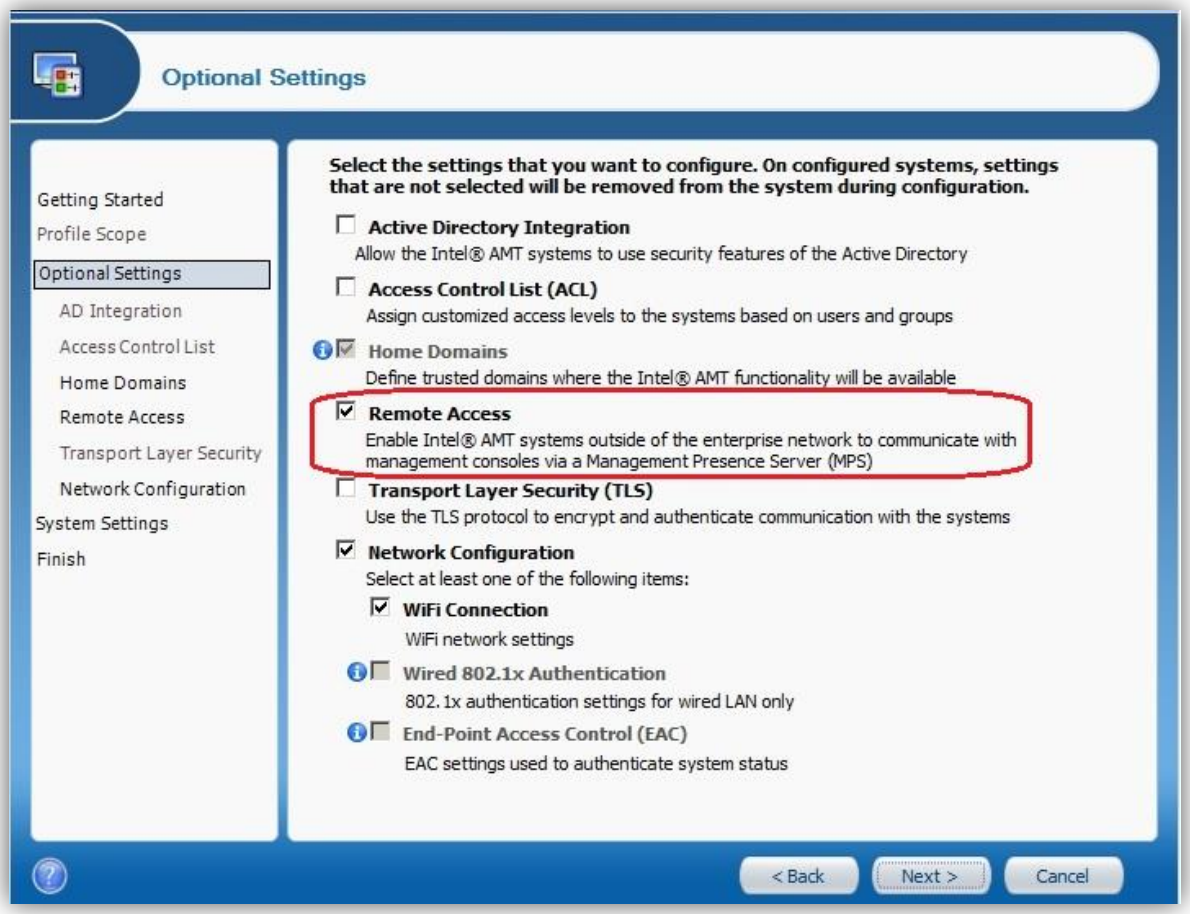



**Ilustración 12. Configuración general ACU Wizard**

ACU Wizard permite crear perfiles de provisionamiento. Con este mecanismo se consigue generar diferentes patrones para configurar AMT en los equipos de la empresa, por ejemplo, ordenadores sobremesa (que no vayan a utilizar *Fast Call For Help*) y portátiles.

Se comienza dando un nombre al perfil, y después escogiendo las opciones principales del perfil. En nuestro caso, para provisionar el equipo cliente, elegiremos la opción de *Remote Access* para que se pueda configurar la comunicación con el servidor MPS. Además, permitiremos que se establezca conexión mediante red inalámbrica seleccionando las opciones *Network Configuration* y *WiFi Connection*.

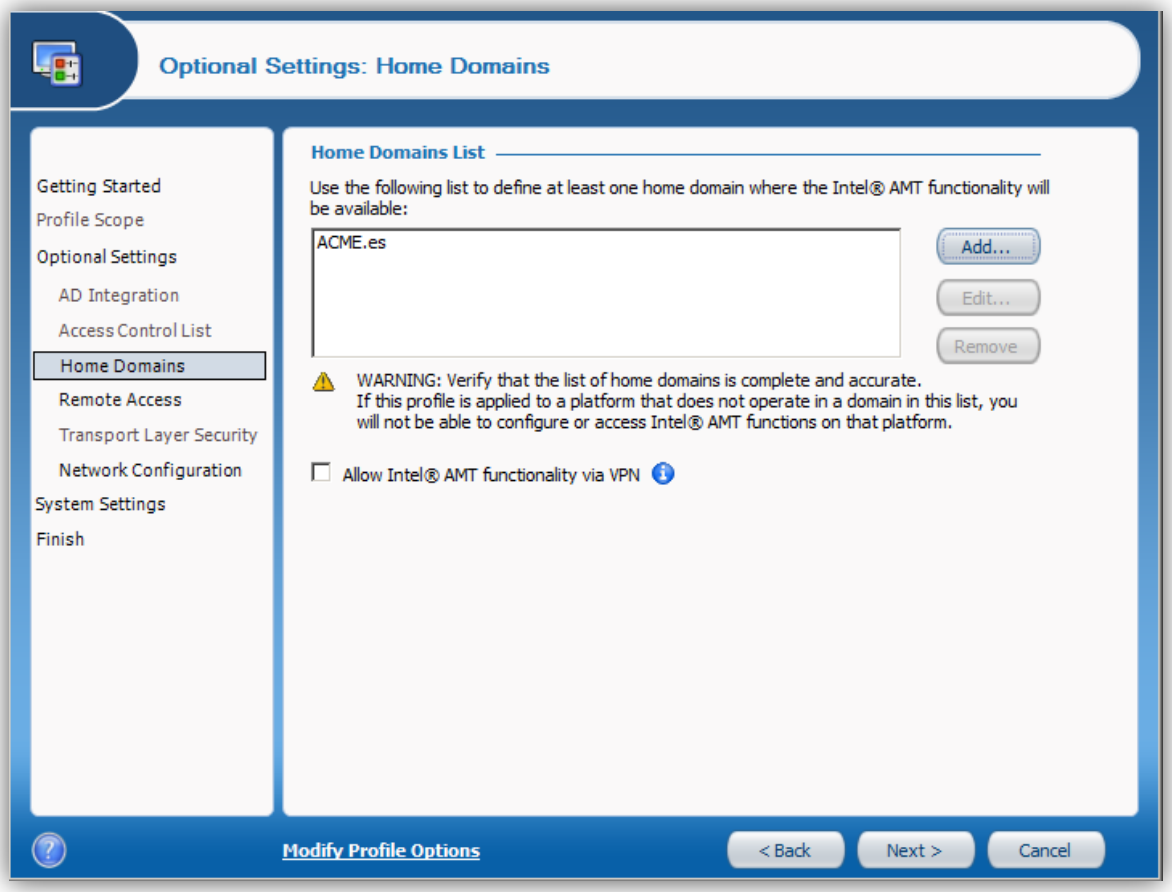



**Ilustración 13. Configuración Home Domains**

El siguiente paso es establecer el dominio interno de la empresa al que el equipo accederá una vez establecida la comunicación con el servidor MPS. En este caso y por cuestiones de privacidad del cliente real, hemos puesto un ejemplo ficticio: ACME.es.

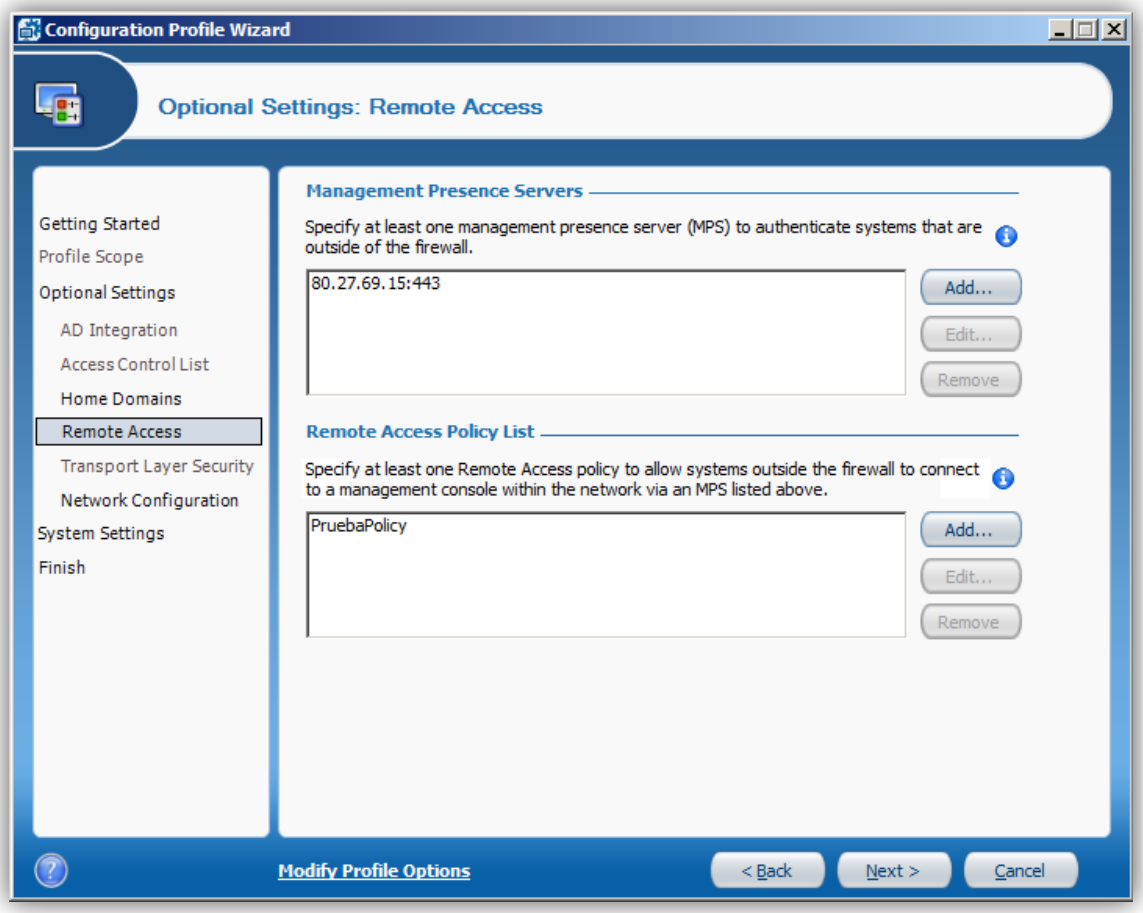



**Ilustración 14. Configuración de acceso remoto**

En el siguiente paso configuraremos los distintos servidores MPS que estarán disponibles para solicitar asistencia remota. Aquí pondremos la dirección IP pública de la interfaz de Stunnel de cara al exterior de la red, para poder ser localizada por los equipos cliente. La dirección IP especificada es la 80.27.69.15, y el puerto designado para la conexión es el puerto SSL por defecto, 443.

En la misma pantalla se puede configurar las políticas de acceso remoto. Nosotros hemos creado una de nombre “PruebaPolicy”, de la cual veremos la configuración más adelante.

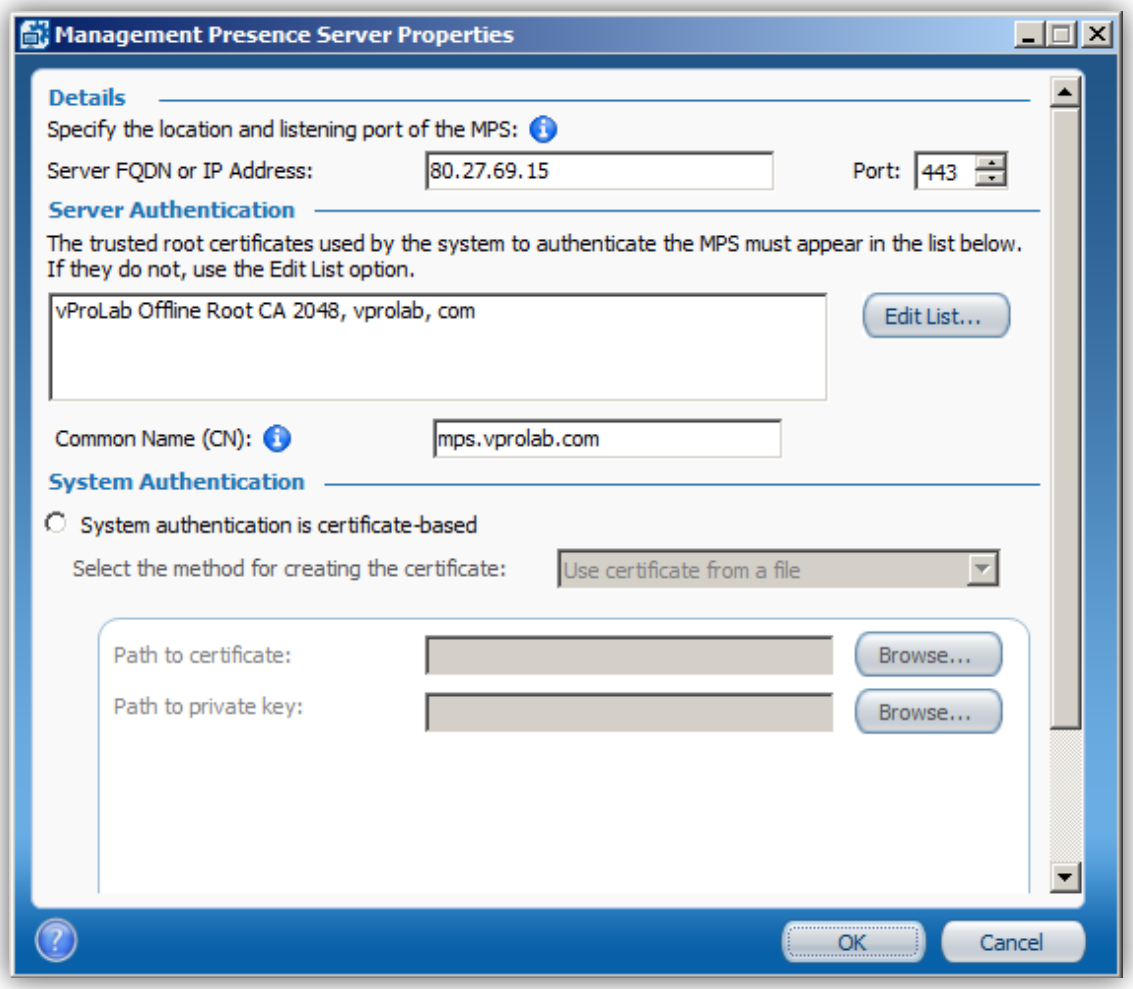



**Ilustración 15. Configuración propiedades MPS**

Esta es la pantalla de configuración de un servidor MPS. Aquí establecemos la dirección IP pública mencionada anteriormente, junto con el puerto que escuchará las llamadas, los certificados raíz usados por el sistema para autenticar el servidor MPS, el nombre que designa el servidor (*Common Name*) y el tipo de autenticación del cliente.

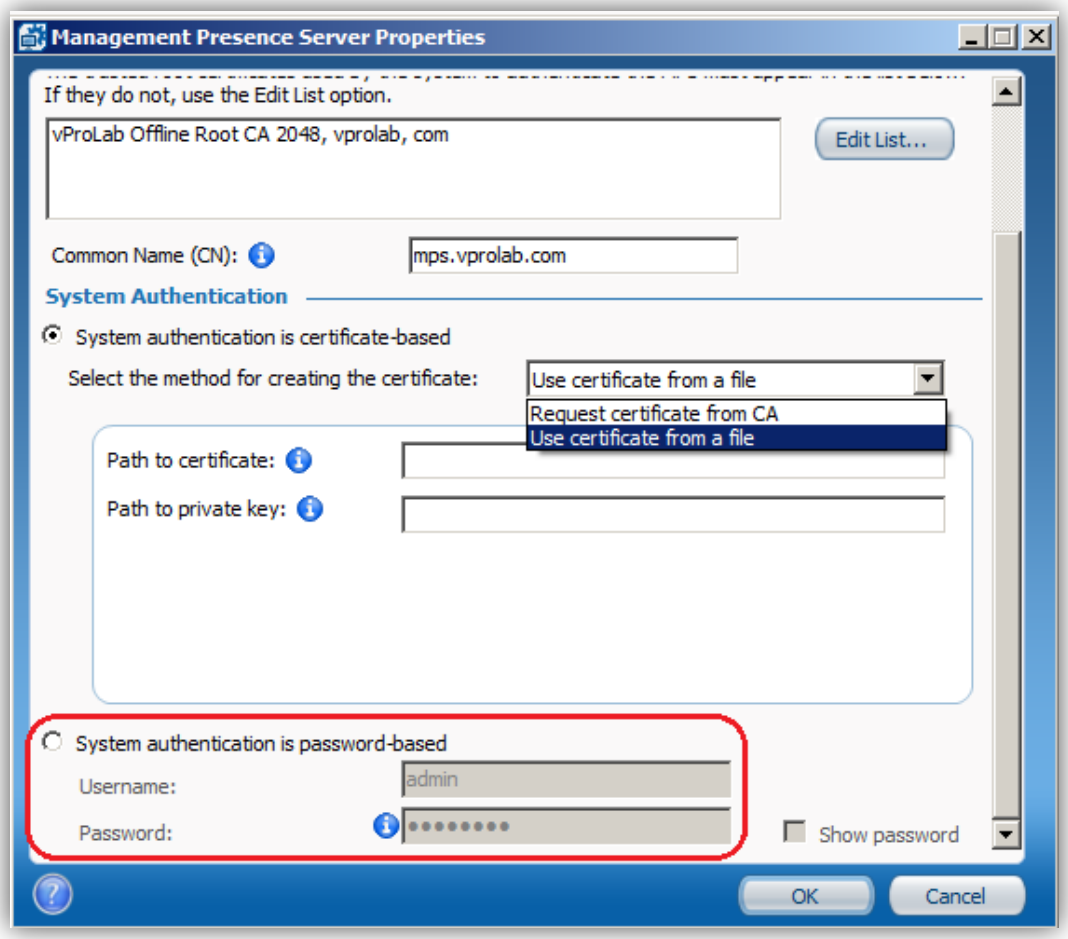



**Ilustración 16. Configuración autenticación cliente**

Para este Proyecto no usaremos un certificado en el cliente, sino que emplearemos el método de autenticación de usuario y contraseña.

Como se puede observar, si se optara por la validación mediante certificado, es posible solicitarlo a una Autoridad de Certificación o seleccionarlo de un fichero, si ya tuviéramos uno en el equipo. Este método es conveniente para empresas que opten por una mayor seguridad a la hora de desplegar el entorno *Fast Call For Help*.

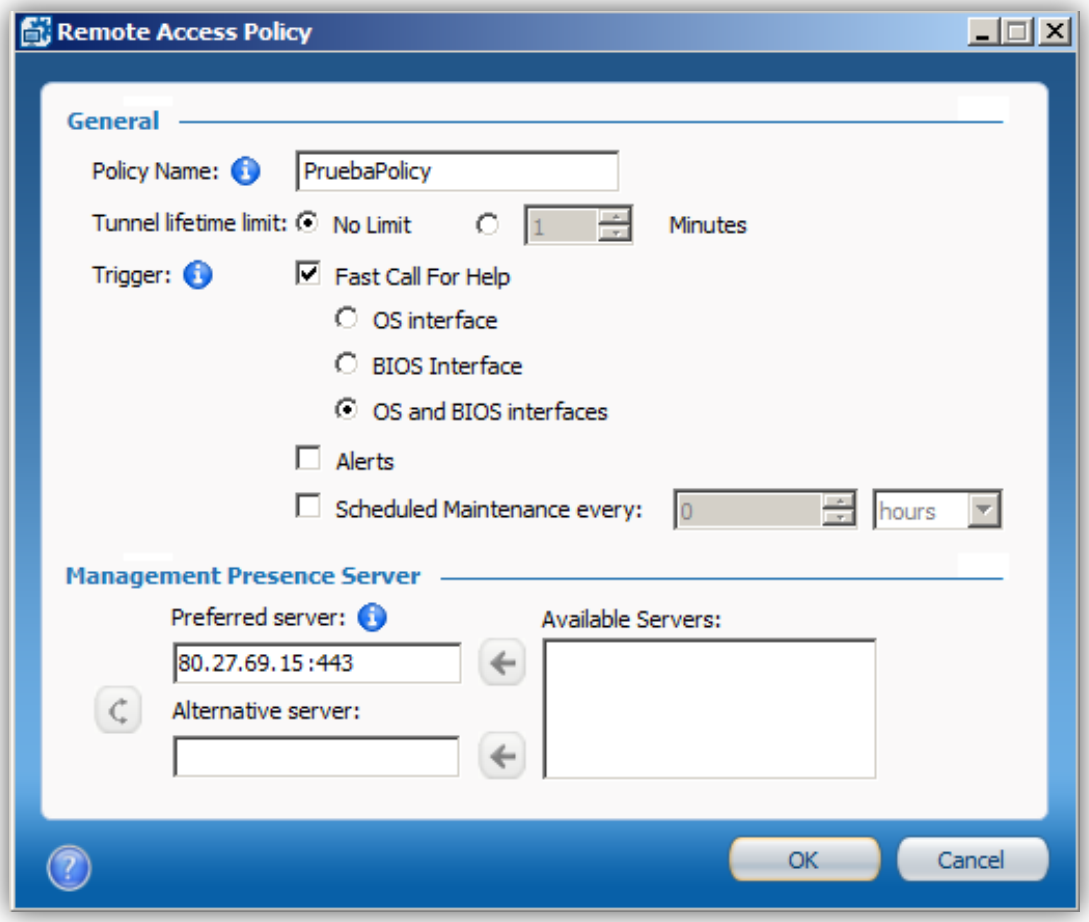



**Ilustración 17. Configuración de la política**

En la pantalla de configuración de la política de acceso remoto se puede establecer, entre otras cosas, el nombre de la política, la duración limitada del túnel establecido durante la comunicación, el tipo de interfaz que se mostrará durante la conexión de la consola al equipo cliente (sólo BIOS, sistema operativo o una combinación de ambos), y la dirección IP del servidor MPS al que se aplicará dicha política.

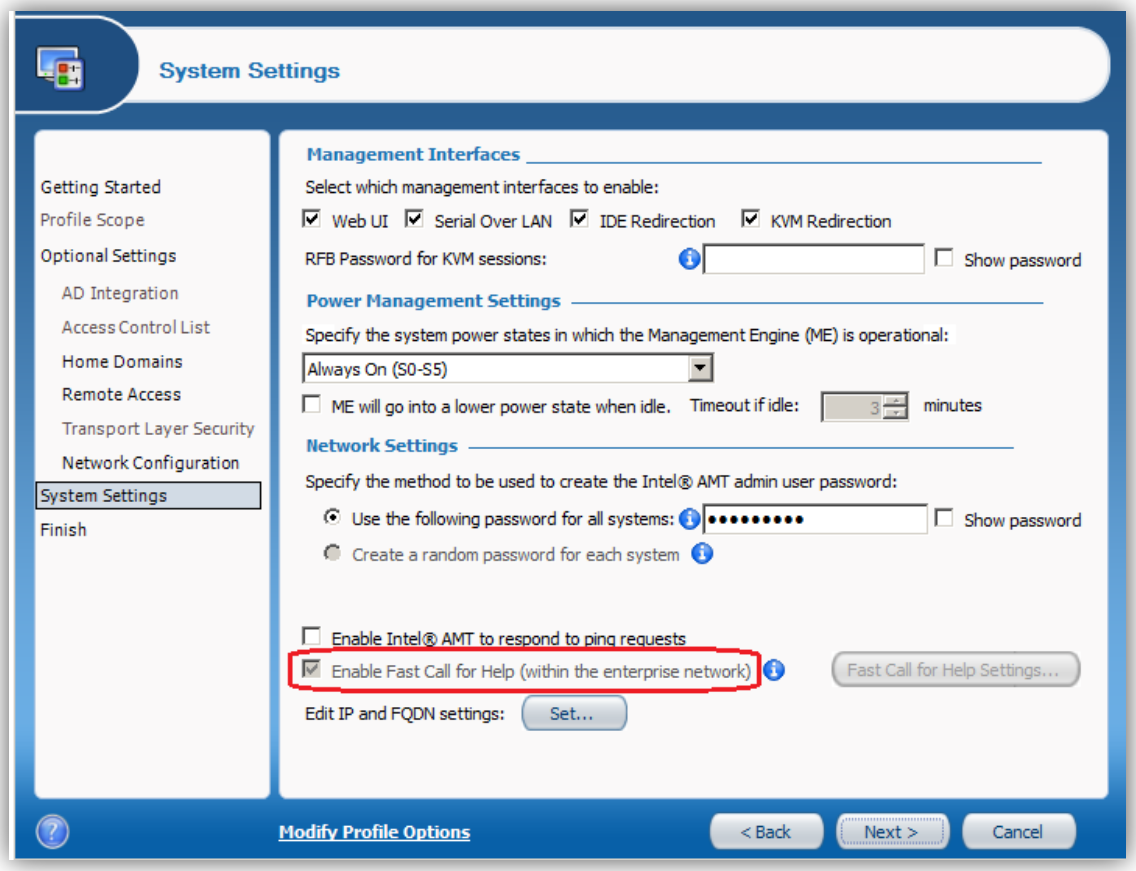



**Ilustración 18. Configuración resumen**

En esta última pantalla de configuración se muestra las opciones de la conexión remota. En nuestro caso hemos habilitado la interfaz web (una sencilla manera de gestionar un equipo, pero con posibilidades limitadas), el protocolo Serial Over LAN, la redirección IDE y la redirección KVM para sesiones de control remoto con interfaz gráfica. Además, aparecerá marcada por defecto la casilla de "Habilitar Fast Call For Help (dentro de la red corporativa), ya que hemos configurado los parámetros de esta tecnología en pasos anteriores.

## 4.3. Consola de gestión

La parte del entorno *Fast Call For Help* que controlará remotamente los equipos que hayan solicitado la asistencia no necesita una configuración especial. Simplemente, instalaremos la herramienta Manageability Commander Tool, disponible en el paquete de software Intel Developer Toolkit v6.0.10314, en el equipo que deseemos que actúe de consola y configuraremos las conexiones.

Después de haber instalado el programa, procedemos a agregar un MPS para que se comunique con él y reciba las solicitudes de asistencia. Estableceremos como puerto HTTP el 8080 y como puerto SOCKS el 8090.

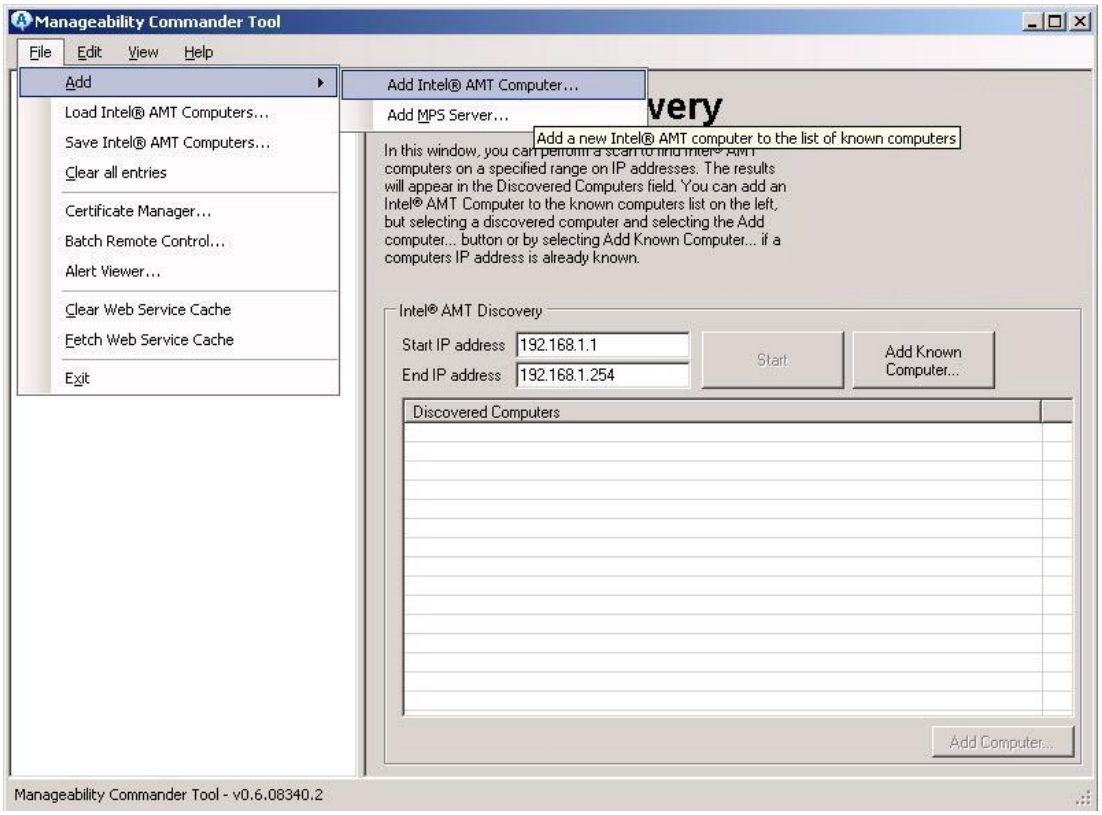



**Ilustración 19. Agregar MPS en Commander**

Una vez añadido, hay que especificar el equipo o equipos que queremos que sean gestionados remotamente, y de los cuales podremos recibir las solicitudes mencionadas anteriormente. Si no se añaden los equipos manualmente la consola de gestión no reconocerá las llamadas y, por lo tanto, no se podrá conectar a los equipos. En nuestro caso, agregaremos un equipo mediante su *hostname* "thinkpad" (por ser un modelo Thinkpad de Lenovo), establecido en la configuración AMT del cliente. Además, al añadir un equipo se nos pedirá el usuario y contraseña de la configuración AMT, ya que el administrador de TI se necesitará dichos permisos para poder gestionar de forma remota el equipo.

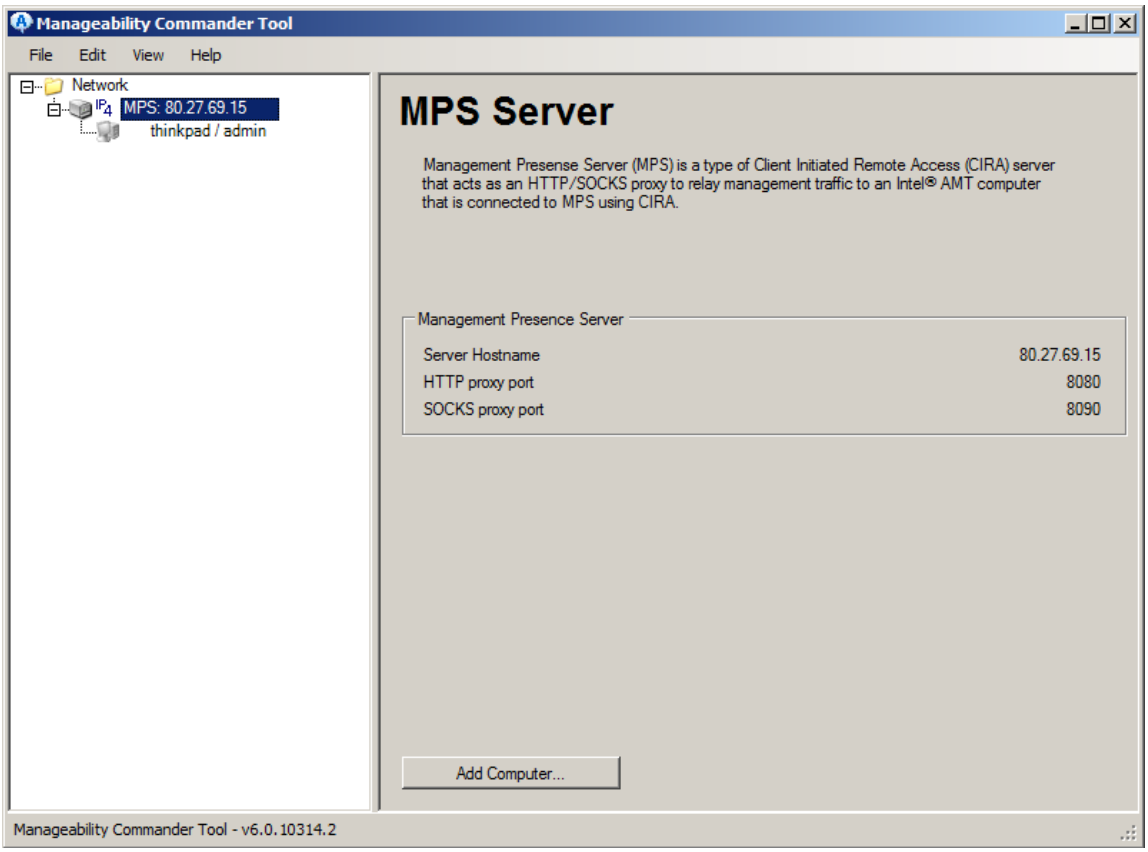



**Ilustración 20. MPS añadido**

Cuando el equipo cliente ya se encuentra colgando del servidor MPS en el listado de *Commander*, la consola de gestión ya está lista para recibir solicitudes de asistencia de ese cliente, redirigidas por el servidor Apache.

# **Capítulo 5.** Pruebas del sistema

En este apartado se presenta la batería de pruebas realizadas al entorno una vez implantado, para comprobar su correcto funcionamiento.

Para describir cada prueba se va a utilizar la siguiente plantilla:

| **Identificador** | P-XX |
|---|---|
| **Objetivo:** | |
| **Requisitos** | |
| **Desarrollo:** | |
| **Resultado** | Satisfactorio / Fallido |

**Tabla 28. Modelo de tabla para las pruebas**

En el apartado "Identificador" asignaremos un número a cada prueba, comenzando desde el 01 y precedido de la letra "P", que indica que es una prueba.

En el campo "Objetivo" especificaremos cuál es la finalidad de la prueba.

En el apartado "Requisitos" se concreta qué será necesario configurar o realizar para a la ejecución de la prueba.

En el campo "Desarrollo" se detalla el proceso de la prueba indicando, en su caso, las configuraciones mencionadas en el apartado "Requisitos".

En el campo "Resultado" puede aparecer "Satisfactorio" o "Fallido", en función del éxito de la prueba.

## 5.1. Pruebas de aceptación

| Identificador | P-01 |
|---|---|
| **Objetivo:** | El cliente debe conectar con la consola antes de arrancar el sistema operativo |
| **Requisitos** | Ninguno |
| **Desarrollo:** | El equipo cliente, ante una situación de inoperatividad, pulsa una tecla para establecer una conexión con la consola de gestión. El resultado de esa llamada debe reflejarse en dicha consola como "conexión establecida". |
| **Resultado** | Satisfactorio |

**Tabla 29. P-01. Conectar estando fuera del sistema operativo**

| Identificador | P-02 |
|---|---|
| **Objetivo:** | El cliente debe conectar con la consola después de arrancar el sistema operativo |
| **Requisitos** | Tener el sistema operativo funcionando |
| **Desarrollo:** | El equipo cliente, ante una situación de inoperatividad, hace clic en el botón correspondiente del software de AMT para establecer una conexión con la consola de gestión. El resultado de esa llamada debe reflejarse en dicha consola como "conexión establecida". |
| **Resultado** | Satisfactorio |

**Tabla 30. P-02. Conectar estando dentro del sistema operativo**

| Identificador | P-03 |
|---|---|
| **Objetivo:** | Apagar el equipo |
| **Requisitos** | Ninguno |
| **Desarrollo:** | Estando el equipo cliente en cualquier situación fuera del sistema operativo, como por ejemplo dentro de BIOS, después de haber pasado una herramienta de testeo de memoria o un antivirus, se podía enviar un comando desde la consola de gestión para apagar el equipo de forma remota. El efecto es el mismo que si se mantuviera pulsado el botón de encendido/apagado del equipo para cortar la corriente que alimenta la placa base. |
| **Resultado** | Satisfactorio |

**Tabla 31. P-03. Apagar el equipo**

| Identificador | P-04 |
|---|---|
| **Objetivo:** | Encender equipo y monitorizar POST |
| **Requisitos** | Si se desea realizarla bajo entorno gráfico, es necesario establecer una sesión KVM. |
| **Desarrollo:** | A través de la interfaz de la Manageability Commander Tool, al enviar una señal SoL desde la consola de gestión estando el equipo cliente apagado, se encendía correctamente. Desde la misma interfaz de la aplicación MCT, sin necesidad de iniciar ninguna sesión KVM, se podía ver el arranque de forma remota, monitorizando el proceso de POST (*Power-On Self Test*) y pudiendo acceder a las opciones previas al arranque del sistema operativo, como pueden ser el acceso a BIOS, el arranque en modo seguro, o el ***prompt*** para elegir el dispositivo de arranque. |
| **Resultado** | Satisfactorio |

**Tabla 32. P-04. Encender equipo y monitorizar POST**

| Identificador | P-05 |
|---|---|
| **Objetivo:** | Enviar imagen ISO remota |
| **Requisitos** | Disponer de un archivo de imagen ISO en la consola de gestión |
| **Desarrollo:** | Disponíamos de varias imágenes ISO en el equipo que tenía instalada la consola de gestión. Una de ellas era el disco de arranque Hiren's Boot CD v8.7 (67.780 KB) o una imagen de floppy para arrancar en modo MS-DOS (1.440 KB). Ambas se enviaron correctamente a través de la red mediante un comando IDE-R y el equipo cliente arrancó desde ellas, tal y como si tuviera un disco o disquette insertado localmente. |
| **Resultado** | Satisfactorio |

**Tabla 33. P-05. Enviar imagen ISO remota**

| Identificador | P-06 |
|---|---|
| **Objetivo:** | Arrancar desde CD/DVD/floppy local |
| **Requisitos** | Disponer de un medio arrancable insertado en el equipo cliente. |
| **Desarrollo:** | Si el equipo cliente dispone de un medio externo arrancable *(bootable)* se podrá seleccionar desde la consola de gestión para iniciar el arranque desde dicho medio. |
| **Resultado** | Satisfactorio |

**Tabla 34. P-06. Arrancar desde CD/DVD/floppy local**

| Identificador | P-07 |
|---|---|
| **Objetivo:** | Pantallazo azul en el equipo cliente |
| **Requisitos** | Para la simulación es necesario configurar el equipo cliente previamente a la prueba, como se indica a continuación. |
| **Desarrollo:** | Creamos una entrada en el registro de Windows para poder forzar un pantallazo azul *(BSOD, Blue Screen Of Death)* en el equipo cliente y así poder demostrar que era posible establecer una sesión de asistencia remota estando fuera del sistema operativo. El modo de conseguir esto es creando una entrada en la siguiente ruta del registro de Windows:<br>**HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/i8042prt/parameters**<br>Creamos una nueva entrada con clic derecho -> Add value. Le damos el nombre "CrashOnCtrlScroll" y que sea de tipo "RegDword" con valor "1". Para deshabilitar el reinicio automático del sistema al detectar el pantallazo azul, hay que acceder a las propiedades avanzadas del sistema con clic derecho en "My Computer", System Protection, Advanced Options y Startup and recovery. Ahí se desactiva el reinicio automático ante un error del sistema, de manera que cuando suceda, el equipo muestre indefinidamente la pantalla azul con el error, a la espera de que el administrador de TI se conecte al equipo cliente. Para forzar el pantallazo en el cliente, una vez realizados estos cambios es necesario reiniciar y, una vez de vuelta en el sistema operativo, mantener pulsada la tecla Control y pulsar dos veces la tecla Scroll Lock.<br>Una vez forzado este error, el administrador de TI se conecta al equipo y puede observar el código del mismo para poder diagnosticar el fallo. |
| **Resultado** | Satisfactorio |

**Tabla 35. P-07. Pantallazo azul en el equipo cliente**

| Identificador | P-08 |
|---|---|
| **Objetivo:** | Arrancar desde USB remoto |
| **Requisitos** | Debe haber una unidad USB autoarrancable insertada en el equipo cliente. |
| **Desarrollo:** | El cliente dispone de una memoria USB con una serie de herramientas de primeros auxilios (o una imagen limpia del sistema operativo para poder reinstalarlo desde la cual se puede arrancar en caso de avería. Se le solicitó al cliente que introdujera la memoria USB en el ordenador, se encendió el equipo cliente de forma remota y se escogió esta unidad en las opciones de arranque para que el equipo iniciara desde este dispositivo. |
| **Resultado** | Satisfactorio |

**Tabla 36. P-08. Arrancar desde USB remoto**

| Identificador | P-09 |
|---|---|
| **Objetivo:** | Arranque desde partición de recuperación en equipo cliente |
| **Requisitos** | El equipo cliente debe disponer de una partición con un sistema operativo de recuperación. |
| **Desarrollo:** | Al arrancar el equipo cliente, desde las opciones de arranque del sistema (pre-sistema operativo), seleccionamos la partición objetivo, que el equipo reconoce como un disco duro distinto, y carga los archivos desde ahí. |
| **Resultado** | Satisfactorio |

**Tabla 37. P-09. Arranque desde partición de recuperación en equipo cliente**

| Identificador | P-10 |
|---|---|
| **Objetivo:** | Iniciar en BIOS automáticamente |
| **Requisitos** | Ninguno |
| **Desarrollo:** | Hay una opción en la consola Manageability Commander Tool que permite reiniciar el equipo e introducirse en BIOS directamente, sin tener que pulsar ninguna tecla. |
| **Resultado** | Satisfactorio |

**Tabla 38. P-10. Iniciar en BIOS automáticamente**

| Identificador | P-11 |
|---|---|
| **Objetivo:** | Iniciar en BIOS manualmente |
| **Requisitos** | Ninguno |
| **Desarrollo:** | Esta vez tratamos de pulsar la tecla “Suprimir” para entrar en BIOS antes de que arrancara el sistema operativo pero no pudimos lograrlo. Quizá se deba a los ligeros retardos que hay entre que se envía un comando o se pulsa una tecla, y el equipo cliente lo recibe. |
| **Resultado** | Fallido |

**Tabla 39. P-11. Iniciar en BIOS manualmente**

| Identificador | P-12 |
|---|---|
| **Objetivo:** | Iniciar una sesión KVM |
| **Requisitos** | Ninguno |
| **Desarrollo:** | Debido a que los propios equipos con vPro traen integrado un servidor VNC, pudimos establecer una sesión KVM remota mediante la propia consola de gestión para poder monitorizar el arranque del equipo bajo un entorno gráfico, y posteriormente manejar dicho equipo con teclado y ratón, como si estuviera delante del mismo. |
| **Resultado** | Satisfactorio |

**Tabla 40. P-12. Iniciar una sesión KVM**

## 5.2. Matriz de trazabilidad

La matriz de trazabilidad indica qué requisitos son los que se comprueban con cada prueba de aceptación realizada, estableciendo una correlación entre ellos.

| Req. / Prueba | RF-01 | RF-02 | RF-03 | RF-04 | RF-05 | RF-06 | RF-07 | RS-01 | RS-02 | RS-03 | RS-04 | RS-05 | RS-06 | RS-07 | RS-08 | RS-09 | RH-01 | RH-02 | RH-03 | RH-04 | RH-05 | RH-06 | RR-01 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| 02 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| 03 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | X |
| 04 | X | X | X | X | X | X | | | X | X | X | X | X | X | X | X | X | X | | X | X | X | X |
| 05 | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | X |
| 06 | X | X | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | X |
| 07 | X | X | | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | X |
| 08 | X | X | | | | X | X | X | X | X | X | | | X | X | X | X | X | | X | X | X | X |
| 09 | X | X | | | | | X | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | X |
| 10 | X | X | | | | | | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | X |
| 11 | X | X | | | | | | | X | X | X | X | X | X | X | | | | | X | X | X | X |
| 12 | X | X | | | | | | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |

# Capítulo 6. Gestión del Proyecto

## 6.1. Metodología de trabajo

Para la realización del Proyecto Fin de Carrera se ha utilizado un ciclo de vida en cascada realimentado. Esto se debe a que, una vez pasadas las etapas de análisis de requisitos, diseño, etc., se procedía a implantar el entorno y siempre había que hacer correcciones en etapas anteriores para conseguir que funcionara correctamente. Puesto que la documentación de la que disponíamos no era muy completa, hubo que realizar pruebas de 'ensayo y error', que daban a lugar a numerosas iteraciones con las que se conseguía arreglar fallos y provocar unos nuevos.

El modelo en cascada realimentado resulta muy atractivo, hasta ideal, si el proyecto presenta alta rigidez (pocos o ningún cambio, no evolutivo), los requisitos son muy claros y están correctamente especificados. En este caso, el proyecto establece unos requisitos y unas funcionalidades muy claras, que no están sujetas a cambios. Es por ello que hemos decidido aplicar este modelo al desarrollo del mismo.

Se han establecido las siguientes fases de desarrollo del proyecto: preanálisis, análisis, diseño, pruebas, implementación y mantenimiento. Al finalizar cada una de ellas con sus correspondientes tareas, establecimos un hito que indicara que la fase había llegado a su fin.

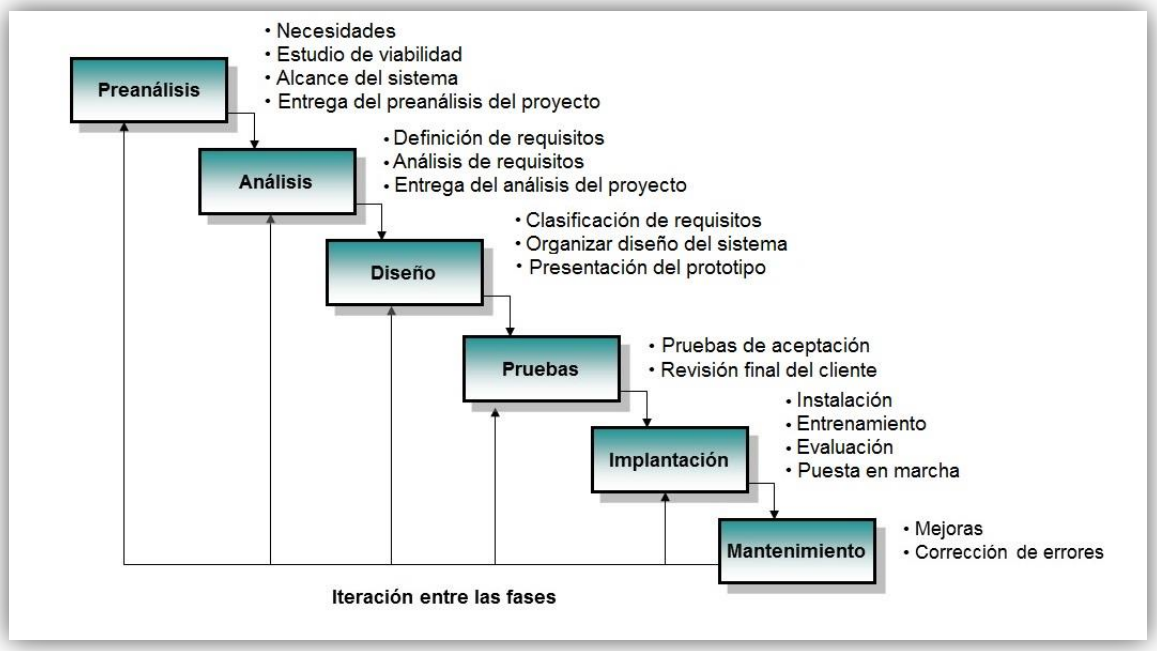
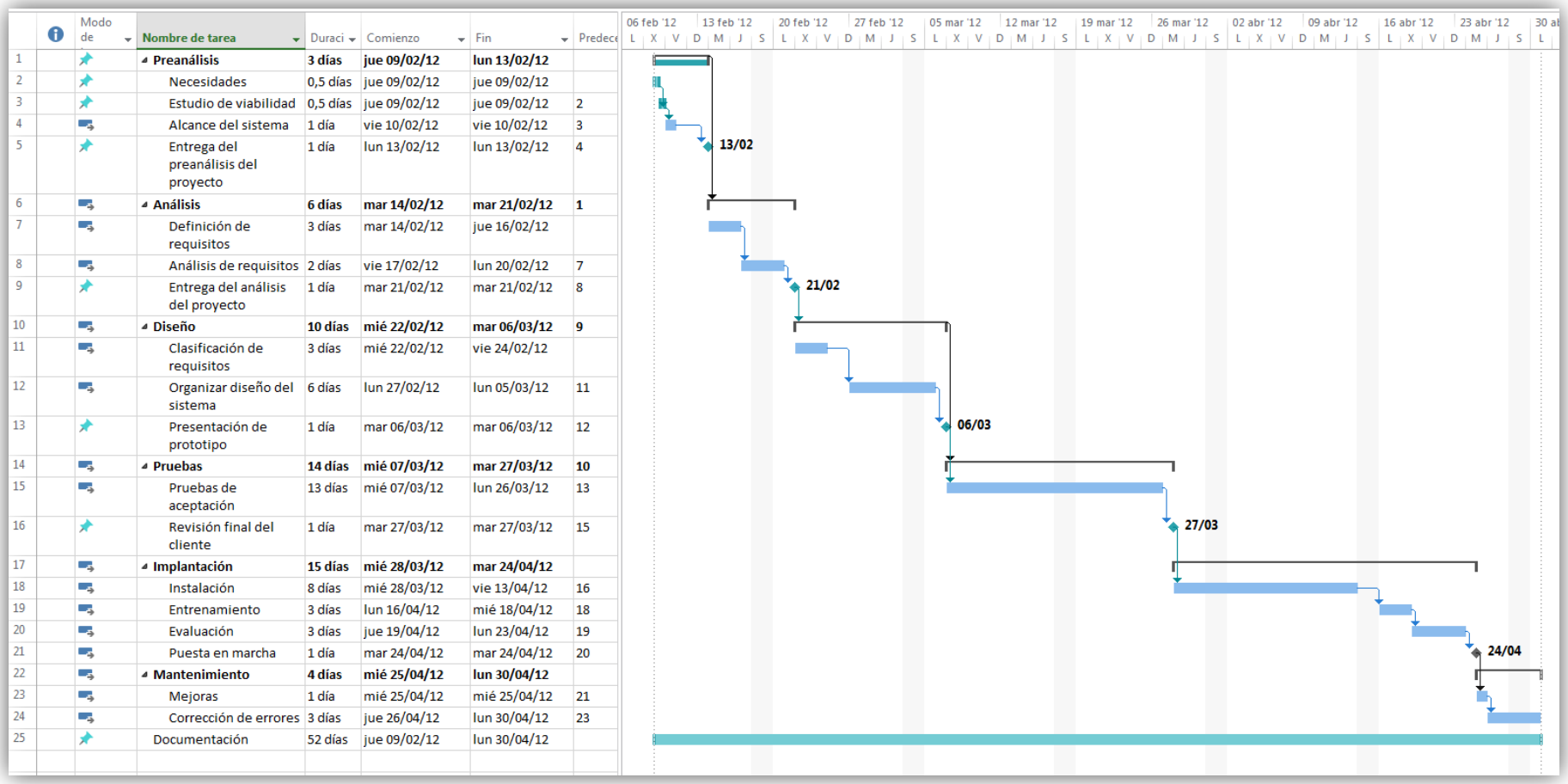



**Ilustración 21. Ciclo de vida en cascada realimentado**

Como hemos comentado anteriormente, aunque los requisitos estaban claros, había partes de la configuración del entorno que no estaban correctamente especificadas y había que retroceder un paso para averiguar dónde podía estar fallando la implementación. Es por ello que este modelo es el que se adapta perfectamente al desarrollo de este Proyecto Fin de Carrera.

## 6.2. Planificación del proyecto. Diagrama de GANTT



| | Modo de | Nombre de tarea | Duraci | Comienzo | Fin | Predec |
|---|---|---|---|---|---|---|
| 1 | | **Preanálisis** | **3 días** | **jue 09/02/12** | **lun 13/02/12** | |
| 2 | | Necesidades | 0,5 días | jue 09/02/12 | jue 09/02/12 | |
| 3 | | Estudio de viabilidad | 0,5 días | jue 09/02/12 | jue 09/02/12 | 2 |
| 4 | | Alcance del sistema | 1 día | vie 10/02/12 | vie 10/02/12 | 3 |
| 5 | | Entrega del preanálisis del proyecto | 1 día | lun 13/02/12 | lun 13/02/12 | 4 |
| 6 | | **Análisis** | **6 días** | **mar 14/02/12** | **mar 21/02/12** | **1** |
| 7 | | Definición de requisitos | 3 días | mar 14/02/12 | jue 16/02/12 | |
| 8 | | Análisis de requisitos | 2 días | vie 17/02/12 | lun 20/02/12 | 7 |
| 9 | | Entrega del análisis del proyecto | 1 día | mar 21/02/12 | mar 21/02/12 | 8 |
| 10 | | **Diseño** | **10 días** | **mié 22/02/12** | **mar 06/03/12** | **9** |
| 11 | | Clasificación de requisitos | 3 días | mié 22/02/12 | vie 24/02/12 | |
| 12 | | Organizar diseño del sistema | 6 días | lun 27/02/12 | lun 05/03/12 | 11 |
| 13 | | Presentación de prototipo | 1 día | mar 06/03/12 | mar 06/03/12 | 12 |
| 14 | | **Pruebas** | **14 días** | **mié 07/03/12** | **mar 27/03/12** | **10** |
| 15 | | Pruebas de aceptación | 13 días | mié 07/03/12 | lun 26/03/12 | 13 |
| 16 | | Revisión final del cliente | 1 día | mar 27/03/12 | mar 27/03/12 | 15 |
| 17 | | **Implantación** | **15 días** | **mié 28/03/12** | **mar 24/04/12** | |
| 18 | | Instalación | 8 días | mié 28/03/12 | vie 13/04/12 | 16 |
| 19 | | Entrenamiento | 3 días | lun 16/04/12 | mié 18/04/12 | 18 |
| 20 | | Evaluación | 3 días | jue 19/04/12 | lun 23/04/12 | 19 |
| 21 | | Puesta en marcha | 1 día | mar 24/04/12 | mar 24/04/12 | 20 |
| 22 | | **Mantenimiento** | **4 días** | **mié 25/04/12** | **lun 30/04/12** | |
| 23 | | Mejoras | 1 día | mié 25/04/12 | mié 25/04/12 | 21 |
| 24 | | Corrección de errores | 3 días | jue 26/04/12 | lun 30/04/12 | 23 |
| 25 | | Documentación | 52 días | jue 09/02/12 | lun 30/04/12 | |



Ilustración 22. Diagrama de Gantt

## 6.3. Presupuesto del proyecto

Para los cálculos de los costes se han tenido en cuenta las siguientes consideraciones:

- La fecha de inicio del Proyecto se establece el 9 de febrero del año 2012 y la fecha de finalización estimada es el 30 de abril de 2012.
- Existe un día festivo, el 19 de marzo, San José, y un periodo vacacional desde el 2 de abril hasta el 6 de abril por Semana Santa. En total, se trabajó 52 días.
- La jornada laboral comprende de lunes a viernes, 8 horas diarias.
- El total de horas trabajadas asciende, por lo tanto, a 416 horas.

### 6.3.1. Cálculo de costes de personal

Para el desarrollo de este Proyecto Fin de Carrera en un entorno real serán necesarios varios papeles, a desemplear por las personas enumeradas en la siguiente tabla y asociadas a las siguientes fases:

| Fase | Rol | Coste por hora (€ / h) | Total horas | Total coste (€) |
|---|---|---|---|---|
| **Preanálisis** | Analista | 50 | 24 | 1.200 |
| **Análisis** | Analista | 50 | 48 | 2.400 |
| **Diseño** | Analista | 50 | 80 | 4.000 |
| **Pruebas** | Técnico | 60 | 112 | 6.720 |
| **Implantación** | Técnico | 60 | 120 | 7.200 |
| **Mantenimiento** | Técnico | 50 | 32 | 1.600 |
| **Documentación** | Técnico | 40 | 40 | 1.600 |
| **TOTAL** | | | **456** | **24.720** |

**Tabla 41. Costes de personal**

### 6.3.2. Costes de hardware

Será necesaria la utilización de dos equipos que se situarán físicamente dentro del entorno empresarial (DMZ y consola) y, como mínimo, otro que será el que utilizará el empleado para ejercer de cliente vPro. En el posible caso de utilizar más de un equipo cliente, habría que multiplicar el coste de adquisición de un equipo con tecnología vPro por cada empleado que fuera a estar asociado al servicio de gestión remota que ofrece la empresa. En este caso, consideraremos sólo uno.

El coste no se calculará mediante amortización limitada al periodo de desarrollo del Proyecto porque se considera que seguirán siendo utilizados posteriormente a su finalización, para dar el servicio para los que se han implantado.

En cuanto a coste de hardware de conectividad, daremos por hecho que las comunicaciones se establecerán entre los distintos componentes del entorno a través de una tarjeta de red inalámbrica, incluida en el presupuesto de cada equipo.

| Concepto | Coste (€) | Unidades | Total (€) |
|---|---|---|---|
| **Equipo consola** | 800 | 1 | 800 |
| **Equipo DMZ** | 2.000 | 1 | 2.000 |
| **Equipo cliente (portátil)** | 800 | 1 | 800 |
| **TOTAL** | | | **3.600** |

Tabla 42. Costes de hardware

### 6.3.3. Costes de software y tecnologías

Tanto en el equipo cliente como en el consola se han usado los Sistemas Operativos que venían preinstalados de fábrica, y que no han tenido un sobrecoste respecto al precio de adquisición de dichos equipos. El sistema operativo es Windows 7 en ambos casos.

En el equipo que soportará la DMZ se ha instalado una máquina virtual con Windows Server 2008 R2 Standard, conseguido de forma gratuita por la alianza de Microsoft y la Universidad Carlos III de Madrid a través del programa MSDN, e instalado a su vez en el software de prueba -gratuito durante un mes- de gestión de máquinas virtuales VMWare Workstation.

El resto de software es gratuito: tanto Apache como Stunnel, Commander, MPS y el editor de texto usado para editar los archivos de configuración, Notepad++, son de libre acceso.

Los certificados digitales pueden ser creados mediante la CA de Microsoft integrada en Windows Server 2008, por lo que no es necesario acudir a una Autoridad de Certificación, ya que los certificados no van a tener ámbito público y sólo se van a usar de modo interno en el ámbito empresarial.

| Concepto | Coste (€) | Unidades |
|---|---|---|
| **Licencia Windows Server 2008 R2 Standard** | 600 | 1 |
| **TOTAL** | | 600 |

Tabla 43. Costes de software y tecnologías

### 6.3.4. Coste total del Proyecto

Para hallar la inversión total del Proyecto, simplemente, sumaremos los costes parciales calculados hasta ahora y añadiremos un margen de beneficio del 40%, un colchón de seguridad del 30% del presupuesto, y el IVA a fecha de redacción de esta documentación (21%).

| Concepto | Coste (€) |
|---|---|
| **Costes de personal** | 24.720 |
| **Costes de hardware** | 3.600 |
| **Costes de software y tecnologías** | 600 |
| **Colchón de seguridad (30%)** | 6.369 |
| **Margen de beneficio (40%)** | 8.492 |
| **IVA (21%)** | 7.579,11 |
| **TOTAL** | **43.670,11** |

Tabla 44. Coste total del Proyecto

# Capítulo 7. Conclusiones

En este capítulo se ofrece una serie de conclusiones técnicas sobre este Proyecto Fin de Carrera, así como una valoración del trabajo realizado y, por último, una proposición de futuras mejoras y líneas de trabajo.

## 7.1. Conclusiones técnicas.

Este es un Proyecto del cual se puede sacar mucho provecho, debido a que las empresas pueden ahora, a través de una inversión en la infraestructura necesaria, gestionar el parque de ordenadores de los que dispongan, independientemente de si se encuentran localizados en el ámbito corporativo o fuera, siempre que dispongan de conexión a Internet y estén conectados a la corriente eléctrica.

Al tratarse de una solución que se basa en la comunicación por hardware, se elimina el problema de que el usuario tenga que estar dentro del sistema operativo para que el administrador pueda establecer una conexión remota, ya que el problema del ordenador cliente puede ser precisamente que no se lance correctamente el sistema operativo, o haya aparecido una pantalla azul de error crítico en Windows, etc.

Uno de los problemas que hemos encontrado, aunque tiene sentido que sea así como se haya configurado el funcionamiento de FCFH, es que el equipo necesita estar conectado a la corriente eléctrica para poder recibir respuesta a su solicitud de ayuda. Esto es así porque la consola de gestión necesita asegurarse de que podrá conectarse al equipo y enviar señales eléctricas al conjunto de componentes que debe tener el equipo para poder soportar las tecnologías que componen vPro (chipset, tarjeta de red

y microprocesador). Una vez hayan llegado las señales eléctricas y los comandos correspondientes a los componentes, el equipo se podrá encender de forma remota y ya se podrá proceder a su diagnóstico.

## 7.2. Valoración del trabajo realizado.

Este proyecto me ha servido para aplicar algunos de los conocimientos adquiridos a lo largo de la carrera, como por ejemplo en el ámbito de la seguridad informática y los certificados digitales.

El proceso de configuración de todo el software fue largo y tedioso. Al no contar con una documentación que detallara el proceso hizo que fuera más complicado de lo esperado. Además, el hecho de no marcar correctamente una opción en cualquiera de los paquetes de software utilizados limitaban la funcionalidad de la tecnología, por ejemplo, impidiendo que se redirigiera la señal de arranque del equipo cliente a la unidad de DVD virtual del equipo consola, o no permitiendo establecer una sesión KVM para poder gestionar el equipo mediante un entorno gráfico.

El esfuerzo realizado ha compensado el haber podido hallar la solución al problema de la gestión remota, sobre todo sabiendo que este entorno puede ayudar a muchas empresas a no interrumpir su proceso productivo por averías o incidencias producidas fuera del entorno empresarial.

## 7.3. Trabajo futuro

Como añadido al trabajo realizado, hemos hecho pruebas con un *smartphone* como medio de acceso a Internet. El propósito de estas pruebas es habilitar, en un futuro próximo, la asistencia al cliente que accede con su portátil a Internet a través de su teléfono móvil con conexión a internet. Para ello ha sido necesario configurar el móvil como punto de acceso a través de WiFi, conectándose éste a su vez a la red a través de 3G. Compartiendo la conexión del teléfono, y estableciendo una conexión segura con el portátil a con un cifrado de tipo WPA2-PSK (WiFi Protected Access 2 – PreShared Key), el portátil puede navegar a través de Internet sin problemas. También es capaz de recibir comandos SoL e IDE-R de la consola de gestión, y por lo tanto arrancar desde imágenes ISO remotamente, al igual que el apagado y encendido remoto, entre otras cosas. Lógicamente, la imagen ISO tiene que ser de unos pocos Megabytes, ya que la velocidad de subida y bajada por 3G no es la misma que por cable o por WiFi y tardaría mucho tiempo en arrancar.

Además, Intel está introduciendo su tecnología vPro en tabletas[4] y probablemente lo haga con teléfonos móviles en un corto periodo de tiempo. De esta manera, si una empresa considera tener estos tipos de dispositivos para uso profesional, podrá gestionarlos de igual manera que hasta ahora hacía con los ordenadores.

- Limitaciones y posibles mejoras en el MPS:

Citando puntos de posibles mejoras por parte de los desarrolladores de la solución, tomamos como ejemplo el MPS. Como hemos visto, es necesario registrar previamente la flota de ordenadores disponibles para poder identificar qué equipo es el que está realizando la solicitud a través de la consola de gestión gratuita de Intel, usada en este Proyecto Fin de Carrera. Esto para las grandes empresas puede suponer un problema de viabilidad si disponen de un parque de equipos muy grande, debido a que se tendría que invertir mucho tiempo y esfuerzo en dar de alta en la base de datos de los equipos de la consola de gestión. Este inconveniente se podría solucionar a través de un servidor DHCP y utilizando consolas de pago con más funcionalidades integradas.

[4] http://www.motioncomputing.com/resources/F5/vPro_Overview.pdf

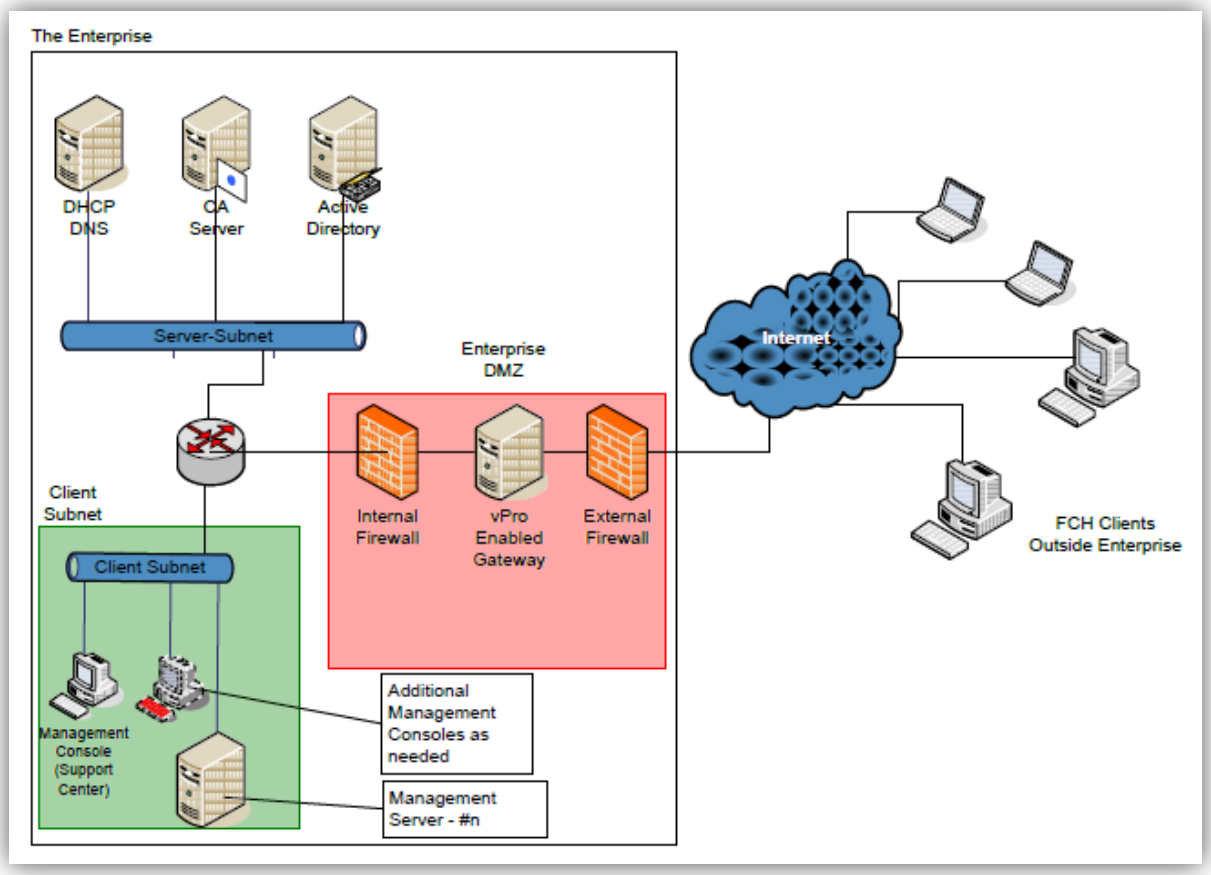



**Ilustración 23. Entorno FCFH con servidores DHCP, DNS, CA y Active Directory**

Además, la interfaz de dicha consola quizá sea un tanto precaria. Sirve para un uso básico, pero es algo incómoda para utilizar el servicio a diario. Convendría rediseñarla y hacerla más atractiva para el usuario.

Otros aspectos susceptibles de revisión en el software y algunas nuevas funcionalidades se podrían habilitar con el soporte de:

- Más conexiones simultáneas: MPS debe soportar una magnitud mayor de conexiones, del orden de miles de ellas. La implementación actual funciona para proyectos pequeños y medianos, pero no es adecuado para un despliegue de miles de equipos. Para ello, es probable que hubiera que encontrar algún modo de repartir dinámicamente las conexiones entrantes entre varios MPS dentro de la DMZ.
- Un protocolo de notificación estándar: los mensajes de notificación actuales del MPS a la consola de gestión usan un protocolo propietario, SOAP. Esta funcionalidad necesita claramente una estandarización para que MPS se pueda utilizar con consolas de gestión de diferentes fabricantes.

- Uso de consolas de gestión en Internet: en esta versión de MPS no se ha contemplado el uso de dichas consolas en un entorno fuera de la empresa, sino que todo el tráfico es redirigido a la red interna.
- Uso de IPv6: de momento, el software MPS no soporta la nueva versión de las direcciones IP, y esto será necesario tarde o temprano ya que supondrán un nuevo estándar en la industria.
- Apagado más "elegante" y soporte de interfaz gráfica: para cerrar el software MPS hay que matar el proceso, no contando con ninguna opción para terminar con su ejecución. Además, sería conveniente implementar una interfaz gráfica (GUI) para ofrecer un modo visualmente más atractivo de configuración y de gestión de la aplicación.

# Bibliografía


[1] http://www.itlibrary.org/index.php?page=Incident_Management (Noviembre 2012)

[2] Wikipedia

- http://en.wikipedia.org/wiki/Desktop_and_mobile_Architecture_for_System_Hardware (Noviembre 2012)
- http://en.wikipedia.org/wiki/Intel_Active_Management_Technology (Noviembre 2012)
- http://en.wikipedia.org/wiki/WS-Management (Diciembre 2012)
- http://en.wikipedia.org/wiki/SOAP_(protocol) (Diciembre 2012)
- http://es.wikipedia.org/wiki/Software (Enero 2013)

[3] Intel ® Sales and Marketing Content Repository (Abril 2012)

[4] http://dmtf.org/standards/dash (Diciembre 2012)

[5] http://sites.amd.com/la/business/it-solutions/it-needs/manageability/Pages/manageability.aspx (Diciembre 2012)

[6] http://www.idg.es/pcworldtech/Arquitectura-de-administracion-remota-de-equipos/art192330-comunicaciones.htm (Diciembre 2012)

[7] http://communities.intel.com/community/vproexpert (Enero 2013)

[8] http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012.aspx (Enero 2013)

[9] http://www.vproexpert.com/E24VZ/Altiris7/index.html (Diciembre 2012)

[10] http://www.symantec.com/client-management-suite (Diciembre 2012)

[11] http://software.intel.com/en-us/articles/download-the-latest-intel-amt-software-development-kit-sdk/ (Enero 2013)

[12] http://www.verisign.es/ssl/ssl-information-center/ssl-basics/index.html (Diciembre 2012)

[13] http://www.fractaliasystems.com/es (Febrero 2013)

[14] http://msdn.microsoft.com/es-es/library/windows/desktop/aa384470(v=vs.85).aspx (Febrero 2013)

[15] http://kdocs.wordpress.com/2007/02/12/diferencia-entre-wep-y-wpa/ (Enero 2013)

[16] http://www.escomposlinux.org/lfs-es/blfs-es-6.0/postlfs/stunnel.html(Enero 2013)

[17] http://software.intel.com/sites/default/files/m/3/7/7/4/0/8091-Commander_User_Guide_v1.0.pdf (Enero 2013)

[18] https://community.mcafee.com/docs/DOC-3306 (Enero 2013)

[19] http://news.softpedia.com/news/AMD-039-s-Reply-to-Intel-vPro-50320.shtml (Enero 2013)

[20] http://software.intel.com/en-us/articles/intel-vpro-technology-faq (Enero 2013)

[21] http://xca.sourceforge.net/ (Febrero 2013)

[22] http://www.landesk.com/products/management-suite.aspx (Febrero 2013)
[23] http://www.radmin.es/ (Febrero 2013)
[24] http://eswikipediaorgwikisoftware.blogspot.com.es/2010/04/modelo-cascada.html (Febrero 2013)
[25] http://www.taringa.net/posts/info/5855050/Todo-sobre-la-EFI.html (Febrero 2013)
[26] http://communities.intel.com/community/vproexpert/blog/2012/03/20/intel-fast-call-for-help-fcfh-support-in-the-intel-vpro-powershell-module (Marzo 2013)
[27] http://www.realvnc.com/products/viewerplus/1.2/docs/ad1029601.html (Marzo 2013)
[28] http://www.realvnc.com/products/viewerplus/ (Marzo 2013)

# Apéndice I. Glosario de términos, abreviaturas y acrónimos

- ***ACU Wizard (AMT Configuration Utility Wizard)***

  Se trata de un asistente que permite configurar las características del ME sin tener que acceder al MEBx manualmente. Es un software que se ejecuta bajo el sistema operativo y permite gestionar las funcionalidades del ME de una forma sencilla e intuitiva. Viene incluido junto con SCS y se usa para provisionar los equipos mediante HBP.

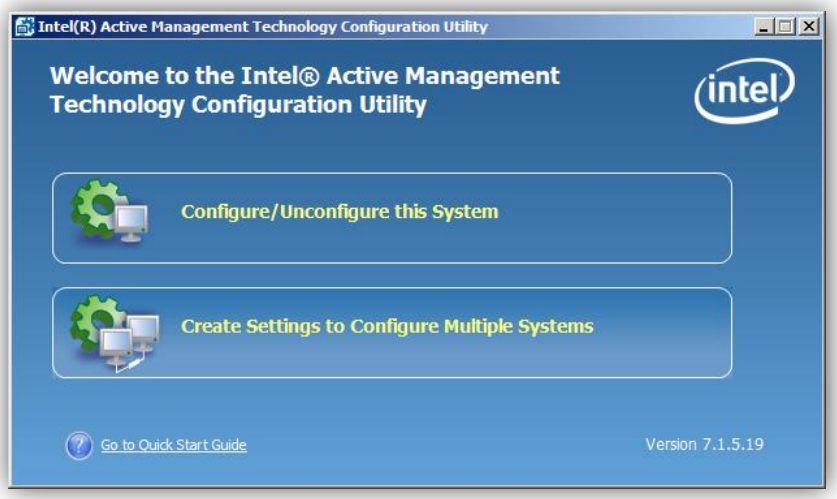



Ilustración 24. ACU Wizard

- ***Apache***

  Se trata de un servidor web de código abierto, formado por una sección core y varios módulos y que, en nuestro Proyecto, permitirá la gestión del tráfico HTTP entre la DMZ y la consola de gestión. El software es gratuito y se puede descargar desde la página web del proyecto Apache[5].

- ***BIOS (Basic Input/Output System)***

  Se trata de una interfaz firmware grabada en la ROM de una placa base de ordenador. Desde aquí se puede acceder a las funciones más básicas de un

[5] http://projects.apache.org/projects/http_server.html

equipo, como es configurar el hardware, habilitar/deshabilitar componentes del sistema, elegir el dispositivo de arranque, etc.
Accediendo a ella se puede habilitar AMT manualmente, en los equipos que tengan esta tecnología integrada.

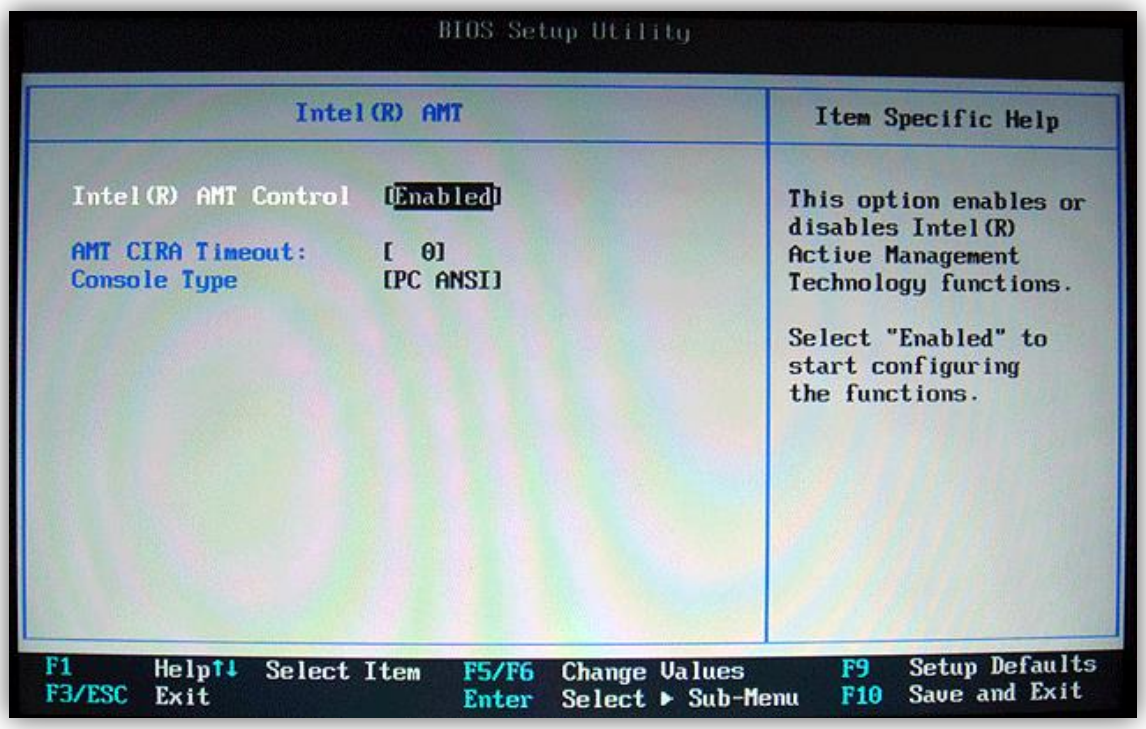



**Ilustración 25. AMT en BIOS**


**Ilustración 26. Prompt *Management Engine***

- ***Certificado digital***

  El certificado digital permite cifrar las comunicaciones. Solamente el destinatario de la información podrá acceder al contenido de la misma. Un certificado digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja. La clave pública forma parte del certificado digital, que es firmado electrónicamente por

una Autoridad de Certificación, una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos del titular.

Otra utilidad de los certificados digitales es que posibilitan el envío de mensajes cifrados: utilizando la clave pública de un certificado, es posible cifrar un mensaje y enviarlo al titular del certificado, que será la única persona que podrá descifrar el mensaje con su clave privada.

- ***DASH (Desktop and Mobile Architecture for System Hardware)***

  Es un estándar, creado por la DMFT y aprobado en 2009, que enumera todos los requisitos necesarios para todos los métodos de gestión remota, tanto a nivel de equipos profesionales como servidores.

- ***DMTF (Distributed Management Task Force)***

  Es el organismo encargado de desarrollar, mantener y fomentar los estándares de gestión de sistemas en el entorno empresarial. Estos estándares permiten la creación de componentes para infraestructuras de gestión de sistemas de forma independiente de la plataforma. De esta manera, creando estándares abiertos, se permite la interoperabilidad de gestión de sistemas de diferentes fabricantes.


**Ilustración 27. Logo DMTF**

- ***DMZ (De-Militarized Zone o Zona Desmilitarizada)***

  Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa -- los equipos en la DMZ no pueden conectar con la red interna. Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna.
  La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS. En nuestro caso, el servidor MPS.

- ***EFI (Extensible Firmware Interface)***

  Se podría definir como la evolución de BIOS con una interfaz gráfica. Su principal inconveniente es la compatibilidad actual: en sistemas operativos Windows está soportada en versiones de servidor para Itanium y las versiones de 64 Bits de Windows Vista SP1 y Windows Server 2008. Esto está cambiando, y la primera marca en incluir EFI en una de sus placas base para el mercado de consumo ha sido ASUS.

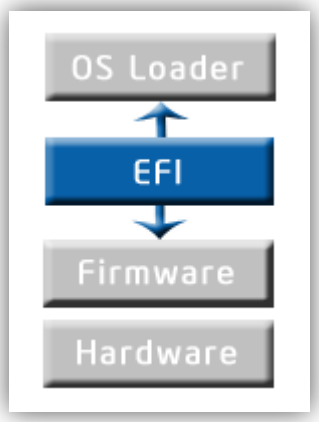



**Ilustración 28. Esquema de situación de la EFI**

- ***FCFH (Fast Call For Help)***

  Es la tecnología propietaria de Intel que permite que sea el equipo cliente el que se solicite la petición de ayuda al administrador de TI, previa a la conexión de este último contra el primero.

- ***Gateway***

  Una puerta de enlace o *gateway* es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su función es traducir la información del protocolo utilizado en la red de origen al protocolo usado en la red de destino.
  Normalmente, es un equipo informático configurado para dotar a las máquinas de una red local conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (*Network Address Translation* o *NAT*).

- ***HBP (Host Based Provisioning)***

  Es un método de provisionamiento y configuración del ME. Como su propio nombre indica, se basa en la configuración local del equipo, sin hacerlo de forma remota a través de una consola, como se haría normalmente en una red corporativa con muchos equipos en el mismo entorno de trabajo.

Cuando se emplea este método, el modo de provisionamiento es "Client Mode", por lo que cada vez que se produzca una conexión contra este cliente se requerirá, por seguridad, el consentimiento del usuario, teniendo que introducir en el equipo que se conecta un código de seis dígitos que aparecerá en la pantalla del equipo cliente.

- ***Intel AMT (Advanced Management Technology*)**

  Se trata de una tecnología de gestión remota integrada en tres componentes de un equipo: microprocesador, tarjeta de red y chipset. Permite la conexión remota a un equipo aunque esté fuera de banda (OOB) y su operabilidad por parte del administrador de TI con una serie de funcionalidades para su gestión. Entre ellas se incluyen el encendido y apagado remoto, redirección de dispositivo de arranque (via IDE-R) y la gestión de otras características de seguridad del equipo cliente.

- ***Intel ME (Intel Management Engine)***

  Intel AMT forma parte de Intel *Management Engine*, el cual es integrado en equipos con soporte de vPro. Es el motor encargado de gestionar la conexión remota entre el equipo cliente y el servidor.

- ***Intel SCS (Setup and Configuration Software)***

  Provee al profesional de TI de las herramientas necesarias para instalar y configurar las características de Intel AMT en equipos con microprocesadores Intel vPro.
  Entre ellas, se encuentran las siguientes:

  - Configuración de red
  - Listas de control de acceso
  - Accesibilidad según el estado de energía del equipo cliente
  - Cableado/inalámbrico
  - Autenticación de red y cifrado
  - Accesibilidad remota a la red

  El paquete SCS se puede descargar de forma gratuita en la página web de Intel[6].

[6] http://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs

- **KVM (*Keyboard*/Video/Mouse)**

  Aunque normalmente se refiere a un switch KVM, en el caso de este Proyecto Fin de Carrera se refiere a una funcionalidad que permite al administrador de TI tener control del equipo remoto a través de una interfaz gráfica que se puede controlar con el ratón y el teclado.

- ***MEBx (Management Engine Bios eXtension)***

  Se trata de la parte del firmware del *Management Engine* que se puede configurar a través de una interfaz gráfica. En él se puede configurar de forma manual los parámetros de un equipo con soporte de la tecnología AMT. Se accede a él a través de una combinación de teclas (normalmente Ctrl + P) antes de entrar en el sistema operativo, habiendo activado el *prompt* previamente en BIOS.


**Ilustración 29. Captura MEBx**

- ***MPS (Management Presence Server)***

  Es un software de libre acceso, creado por Intel, y en nuestro caso es el encargado de gestionar las llamadas de los clientes para dar soporte remoto. Pertenece al SDK de AMT de Intel. Está pensado para ofrecer una herramienta gratuita y sencilla para implementar un servicio de gestión remota para PYMES.

- ***NAT (Network Address Translation)***

  Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles, por pertenecer a diferentes clases. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet. Existen rangos de direcciones privadas que pueden usarse libremente y en la cantidad que se quiera dentro de una red privada. Si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada. De esta manera simultáneamente sólo pueden salir a Internet con una dirección IP tantos equipos como direcciones públicas se hayan contratado. Esto es necesario debido al progresivo agotamiento de las direcciones IPv4. Se espera que con el advenimiento de IPv6 no sea necesario continuar con esta práctica.

- ***Provisionamiento***

  Es el nombre que representa el hecho de activar y configurar AMT en un equipo vPro para poder ser gestionado de forma remota. Hay varias maneras de hacerlo, dependiendo del entorno donde se quiera implantar el servicio, desde un sencillo método a través de una memoria USB en cada equipo que se quiera provisionar, hasta la conexión de los equipos a un servidor de provisionamiento que, tras enviar un certificado de seguridad, enviará al equipo cliente un fichero de configuración con todos los parámetros necesarios.
  En general, los tres modos de provisionamiento son “Basic Mode”, “Standard Mode” y “Advanced Mode”. El primero era conocido previamente como “Client Mode” (o ”SMB Mode”) y los dos últimos pertenecían al antes llamado “Enterprise Mode”. El primero tiene más medidas de seguridad a la hora de recibir una conexión entrante, porque normalmente éste modo es el que se habilita al haber sido provisionado de forma local y no mediante un servidor de provisionamiento con intercambio de certificados. Éste primer modo se utiliza cuando son pocos equipos los que se quieren provisionar, por ejemplo en una PYME. En cambio el segundo y tercer modo, como son para entornos más grandes y que puedan requerir más seguridad a la hora de provisionar.

| Capability | Basic | Standard | Advanced |
|---|---|---|---|
| **Client manageability features** | All | All | All |
| **Client provisioning** | Manual | Automated or manual multiple methods | Automated or manual multiple methods |
| **Required enterprise infrastructure** | DNS and DHCP typical | • DNS and DHCP<br>• Provisioning service | • DNS and DHCP<br>• Provisioning service<br>• Active Directory integration (optional)<br>• Certificate authority (optional) |
| **Client security** | HTTP Digest | HTTP Digest | • HTTP Digest<br>• Kerberos (optional) |
| **Management traffic encryption** | None | None | Digital Certificates (Optional) |
| **Secure network connectivity** | None | None | 802.1X, NAC, NAP (optional) |
| **Client configuration maintenance** | One-to-one | One-to-many | One-to-many |

Ilustración 30. Modos de provisionamiento

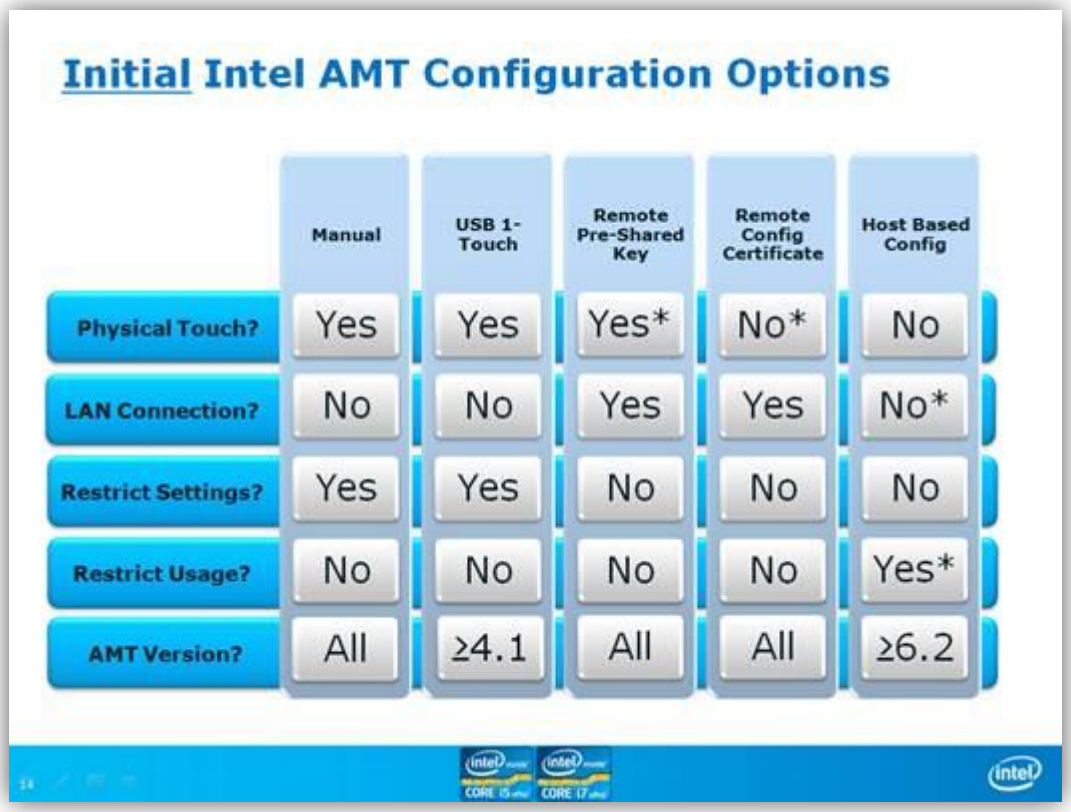



Ilustración 31. Modos de provisionamiento (2)

- ***SDK* (*Software Development Kit* o Kit de Desarrollo de Software)**

  Es generalmente un conjunto de herramientas de desarrollo de software que permite al programador crear aplicaciones para un sistema concreto, por ejemplo ciertos paquetes de software, frameworks, plataformas de hardware,

sistemas operativos, etc. El SDK de Intel que incluye, entre otras herramientas, MPS, se puede descargar de forma gratuita en la página web de Intel[7].

- ***Servidor "blade"***

  Un servidor blade es un tipo de ordenador utilizado, principalmente, en los *data centers*. Ha sido específicamente diseñado para aprovechar el espacio, reducir el consumo y simplificar su explotación.

**Ilustración 32. Ejemplo de servidor blade**

- ***SMASH (Systems Management Architecture for Server Hardware)***

  Es un conjunto de especificaciones que establecen los protocolos estándar para incrementar la productividad en la gestión de un data center.
  El estándar SMASH de DMTF es una suite de especificaciones que enumera la semántica, los protocolos estándar de la industria y los perfiles para unificar la gestión del data center. A través del desarrollo programas de pruebas de conformidad, SMASH podrá extender estas capacidades a infraestructuras multi-plataforma, permitiendo mayor compatibilidad entre servidores de diferentes fabricantes.

- ***SOAP (Simple Object Access Protocol)***

  Es un protocolo diseñado para el intercambio de información estructurada en la implementación de servicios web en redes de ordenadores. Su formato de mensajes se basa en el lenguaje XML (*Extensible Markup Language*), y puede ser utilizado sobre cualquier protocolo de transporte como HTTP, SMTP o TCP.

[7] http://software.intel.com/en-us/articles/download-the-latest-intel-amt-software-development-kit-sdk/

- ***SoL (Serial Over LAN)***

  Serial Over LAN es un mecanismo que permite la entrada y salida de un puerto serie de un sistema gestionado remotamente redireccionado por IP.
  En algunos sistemas gestionados, especialmente servidores de tipo *blade*, los puertos serie normalmente no están conectados a un conector tradicional de puerto serie. Para permitir a los usuarios acceder a las aplicaciones que hay en estos servidores a través del puerto serie, la entrada y salida del puerto serie es redirigida a la red. Por ejemplo, si un usuario quiere acceder a un servidor blade a través del puerto serie, puede hacer telnet a una dirección de red y validarse. En el servidor blade, esta validación se verá como si hubiera sido a través del puerto serie.

- ***SSL (Secure Socket Layer)***

  Es un protocolo criptográfico que proporciona autenticación y privacidad de la información entre extremos sobre internet mediante la criptografía. Habitualmente, sólo el servidor es autenticado, mientras que el cliente se mantiene sin autenticar. En este Proyecto Fin de Carrera se usará para garantizar la conexión segura a través de Stunnel.

- ***Stunnel***

  Se trata de un software que permite crear un túnel cifrado entre dos. Usa el protocolo SSL para cifrar la comunicación entre los dos extremos. En este Proyecto Fin de Carrera lo he utilizado para establecer una conexión segura entre el cliente y la DMZ.
  El software Stunnel se puede descargar de forma gratuita en su página web oficial[8].

- ***Thin clients***

  Es un equipo cliente o un software de cliente en una arquitectura de red cliente-servidor que depende principalmente del servidor central para las tareas de procesamiento, y su función es transportar la entrada y la salida entre el usuario y el servidor remoto. En contraste, un cliente pesado realiza tanto procesamiento como sea posible y trasmite solamente los datos para las comunicaciones y el almacenamiento al servidor.

[8] http://www.stunnel.org

- ***vPro*:**

  Es un término que hace referencia a una serie de tecnologías pensadas para los equipos profesionales, como *Trusted Execution Technology, Anti-Theft* y AMT. Para que los equipos tengan integrada la tecnología Intel vPro, deben contar con un chipset, tarjeta de red y microprocesador Intel certificados. Aunque en el propio producto se muestra la inscripción "vPro" en el adhesivo que indica el procesador que posee el equipo, la lista completa de componentes compatibles con vPro se encuentra en la página web de información de sus productos[9].

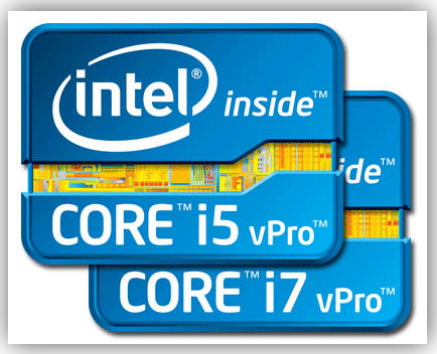



**Ilustración 33. Logo Intel vPro**

- ***WPA (Wi-Fi Protected Access)***

  Es un algoritmo de cifrado de redes inalámbricas. Es la evolución del sistema previo WEP (Wired Equivalent Privacy). WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave precompartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

  WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

[9] http://ark.intel.com

- Para el uso personal doméstico: El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

- Para el uso en empresarial/de negocios: El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS.

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES, *Advanced Encryption Standard*) para el cifrado de los datos, mientras que WPA original emplea TKIP. AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 será compatible tanto con la versión para la empresa como con la doméstica.

- ***WS-MAN (Web Services Management Protocol)***

Este protocolo fue desarrollado por un conjunto de compañías, antes de que en 2005 pasara a pertenecer a la Desktop Management Task Force (DMTF). Está basado en las especificaciones de SOAP, y fue creado con el fin de establecer un estándar público para la gestión remota de cualquier dispositivo que lo integrara.

# Apéndice II. Consolas de gestión remota

A continuación, procederemos a describir brevemente algunas de las consolas de gestión que se encuentran en el mercado y que utilizan grandes empresas actualmente.

Aunque todas están preparadas para gestionar equipos de forma remota mediante Intel vPro, no todas funcionan con *Fast Call For Help*. Por el momento, las únicas que tienen integrada esta tecnología son *McAfee ePO Deep Command*, *Windows PowerShell*, *Real VNC Viewer Plus* y la empleada en el proyecto, *Intel Manageability Commander Tool*.

Algunas de las consolas que soportan la tecnología vPro son:

## Microsoft SCCM (System Center Configuration Manager)

Se trata de la solución de Microsoft perteneciente a la suite System Center, optimizada para Windows, que permite administrar de forma centralizada la configuración de todos los sistemas, físicos y virtuales de una organización. Evalúa globalmente, despliega y actualiza servidores, en equipos cliente y dispositivos ya sean físicos, virtuales, distribuidos y entornos móviles, desde una única consola. Automatiza la gestión de los sistemas (reduciendo costos) y ayuda a los administradores de sistemas a trabajar de forma centralizada.

Configuration Manager ofrece capacidades clave para la gestión de virtualización de escritorio, entrega de aplicaciones (*application delivery)*, gestión de dispositivos y seguridad mientras permite que la productividad vaya paralela a la proliferación de dispositivos.

Entre otras características de administración, se encuentran las siguientes:

- Generación de inventarios, implementación del sistema operativo, administración de actualizaciones evaluación y soporte mejorado para Windows
- Organización de tareas administrativas según roles, permitiendo a los administradores definir una sola vez cada aplicación para entregarla a múltiples dispositivos, reforzando continuamente la configuración para identificar y corregir automáticamente a los equipos que no cumplen con las políticas.
- Administración a través de la consolidación de roles, reducción de la latencia de datos y mejoras de escalabilidad.

## Altiris Client Management Service

Altiris™ Client Management Suite 7.1 de Symantec™ gestiona, securiza y permite solucionar problemas en distintas plataformas, incluyendo Windows®, Mac®, Linux®, y entornos de virtualización de escritorio. Esto permite a las empresas obtener y mantener el control de todo su entorno de TI.

Los administradores de TI suelen tener que desplegar o migrar sistemas, instalar nuevo software o aplicar parches, solucionar incidencias, etc. Esta tarea es, además, más complicada en entornos distribuidos si no se dispone del ancho de banda o recursos adecuados.

Esta solución asegura que se dispone de una infraestructura de gestión robusta que permita gestionar los dispositivos y tareas desde una consola, independientemente de dónde estén localizados los elementos del entorno de TI.

## Fractalia Manager

Fractalia Manager es la solución elegida por las grandes operadoras de telecomunicaciones para ofrecer servicios de gestión remota IT a sus clientes.

Fractalia Manager automatiza servicios de soporte y administración sobre PC, tablets, servidores y smartphones. Permite de una manera muy fácil y sencilla industrializar servicios multicliente sobre cualquier tipo de red. Es capaz de gestionar millones de dispositivos en millones de clientes.

Fractalia Manager dispone de funcionalidades para el soporte y mantenimiento remoto de dispositivos de usuario:

- Soporte Reactivo: atención al cliente remoto en caso de problemas.

- Registro e inventario en plataforma central.
- Chat con operador.
- Control remoto iniciado por el cliente final.
- Solución remota e instantánea ante problemas de disponibilidad del PC.
- Reducción de visitas a casa/oficina de clientes.
- Automatización de tareas para reducir tiempos de respuesta y reparación.

- Soporte Proactivo: mantenimiento de grupos de PC.

- Distribución de aplicaciones software y parches de seguridad.
- Gestión de cambios de inventario hardware y software.
- Control remoto iniciado por el operador.
- Asistencia automatizada y puesta a punto (distribución de SW y aplicaciones, inventariado de equipos, ejecución remota de comandos, etc.)
- Gestión de políticas y operaciones remotas.
- *Integración con Intel vPro para la gestión hardware iAMT.*

## LANDesk Management Suite

Con LANDesk Management Suite se puede:

- Efectuar distribución de paquetes simultáneos a varios usuarios utilizando un mínimo de ancho de banda, sin necesidad de tener hardware dedicado o reconfigurar enrutadores.
- Supervisar las licencias de software de todos los productos desde una perspectiva de licencia o grupo. Administrar varias versiones de productos y reducir los costos de licencias.
- Migrar a Windows 7 u otro sistema operativo en en muy poco tiempo mediante las tecnologías patentadas de Multidifusión dirigida y Servidor preferente.
- Eficiencia empresarial y escalabilidad que administra todos sus servidores centrales en un solo lugar. La interfaz de datos puede sólo mostrar datos que el usuario configure previamente.
- La administración robusta de inventario incluye la detección escalable, vistas detalladas de activos, consola de información fácil de leer y base de datos de inventario integral.
- La administración de energía controla el uso del sistema y el ahorro de energía a nivel de cliente. Identificar los procesos que no deben ser interrumpidos por las políticas de energía.
- Resolución remota del sistema en cualquier momento y lugar. Resolver problemas, generar informes y crear seguimientos de auditoría de forma más sencilla.


**Ilustración 34. Esquema de funcionamiento de LANDesk Management Suite**

## Novell ZENworks

ZENworks 11 SP2 está compuesto por cinco productos que comparten una consola de gestión unificada basada en Web y un solo agente de Adaptive. ZENworks 11 SP2 le proporciona un enfoque único a la gestión de puestos finales basado en el usuario, lo que hace mucho más fácil satisfacer las necesidades de su personal (no solo de los dispositivos que utilizan). Además, con ZENworks 11 SP2, si dispone de uno de los productos, puede activar cualquier otro con tan solo unos clics en la consola de gestión basada en Web, sin necesidad de instalaciones adicionales. Esto incluye:

- ZENworks Configuration Management: Gestión de Endpoint (puesto final), asistencia técnica, y migración a Windows 7 que facilita el trabajo a TI. Obtener más información
- ZENworks Asset Management: Obtenga una idea clara y precisa de todo su hardware y software. Obtener más información
- ZENworks Endpoint Security Management: Gestión de seguridad de puestos finales para proteger sus recursos, evitar las intrusiones malintencionadas y salvaguardar los datos valiosos. Obtener más información
- ZENworks Patch Management: Gestión de parches automatizada hasta para las empresas más exigentes. Obtener más información
- ZENworks Full Disk Encryption: La protección inexpugnable del cifrado completo de discos es ahora fácil de gestionar, incluso en infraestructuras de recursos mixtos (cifrado de hardware y software).

## McAfee ePO (ePolicy Orchestrator) Deep Command

McAfee, al ser propiedad de Intel, ha sido una de las primeras compañías en implementar *Fast Call For Help* en su consola de gestión. Así, al dividirse en distintos módulos con diferentes funcionalidades, *Deep Command* se encargará de gestionar los equipos que tengan activada la tecnología de Intel.

Así es como presenta McAfee su solución de gestión remota con FCFH:

"Cuando se presentan problemas (por ejemplo, un sistema operativo ha sido desactivado o un disco duro ha fallado, tanto administradores como usuarios finales podrán disfrutar de la conveniencia de la administración integrada activada por McAfee ePO Deep Command. Independientemente de si se trata de un PC local o remoto, el administrador puede conectarse al PC desactivado a través de la tecnología Intel AMT para llevar a cabo un arranque remoto desde otra imagen ISO de la red.

La función *Fast Call for Help* de AMT proporciona a los usuarios una forma rápida de ponerse en contacto con los administradores de McAfee ePO para solicitar ayuda. El administrador de McAfee ePO puede rápidamente:

• Redirigir el PC para arrancarlo desde una imagen situada en otra ubicación de la red

• Recopilar datos forenses sobre el malware

• Limpiar y reparar los sistemas infectados, desactivados o puestos en cuarentena sin necesidad de acceder a ellos directamente"


**Ilustración 35. McAfee ePO**

## Microsoft Windows PowerShell

El módulo PowerShell de Intel vPro soporta *Fast Call For Help* a partir de la versión 3.2. Todos los *cmdlets* (extensiones de PowerShell con comandos personalizados) se comunican de manera transparente con el cliente conectado a través de *Management Presence Server.*

Esta nueva característica será de gran utilidad para las empresas que hayan decidido emplear PowerShell para la gestión remota de sus clientes, en lugar de optar por otra consola disponible en el mercado, o si lo usa de forma complementaria a alguna de las mismas.

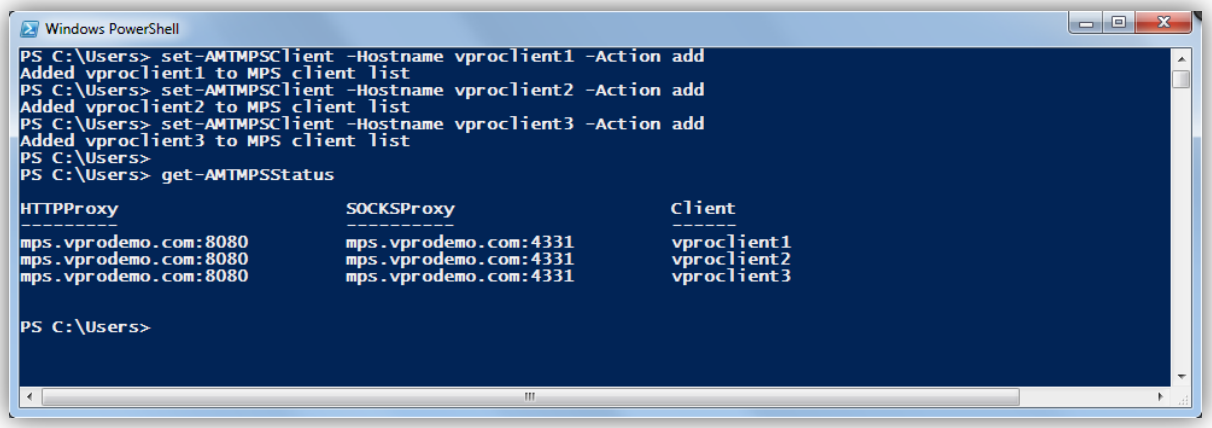



Ilustración 36. Windows PowerShell

## Real VNC Viewer Plus

Con la configuración adecuada del *Management Presence Server*, VNC Viewer Plus puede actuar como consola de gestión en una sesión *Fast Call For Help*, estableciendo automáticamente una conexión segura de vuelta al cliente, y permitiendo al administrador tomar el control del equipo.

El procedimiento de instalar VNC Viewer Plus como consola de gestión depende del MPS, por lo que habría que acudir a la documentación para configurarlo correctamente.

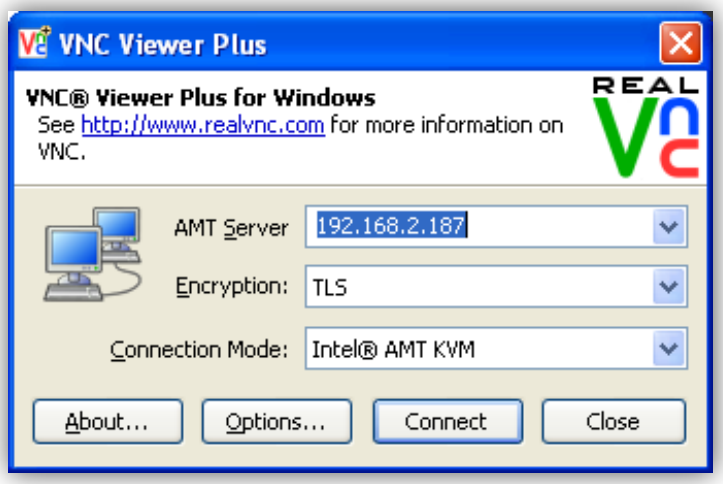



Ilustración 37. VNC Viewer Plus